



# **ShibboLEAP Project**

**Final Report:**

**UCL**

**Martin Moyle  
Adrian Barker**

**May 2006**

<http://www.angel.ac.uk/ShibboLEAP/deliverables/finalreports/ucl.pdf>

## **ShibboLEAP Project Report UCL (University College London)**

### **Authors:**

Martin Moyle

Team Leader, Science, UCL Library Services (Project Coordinator)

Adrian Barker

Section Leader, Internet Technologies, UCL Information Systems (Project Technical Officer)

### **1. Introduction**

#### **1.1. ShibboLEAP**

This report documents UCL's participation in the JISC-funded ShibboLEAP project. The ShibboLEAP project was initiated by the London School of Economics & Political Science (LSE) in response to the JISC Call 11/04 for Early Adopters of Core Middleware for Access Management.

The project aimed to create a Shibboleth Identity Provider (IdP) service at seven of the SHERPA-LEAP (see 1.2) partner institutions to support controlled access to their respective institutional Eprints repositories, both by academic staff acting as depositors, and by library staff acting as editors.

Each of the seven participating SHERPA-LEAP sites uses the open source EPrints2 software platform. ShibboLEAP also aimed to implement modifications to the EPrints2 servers of each of the partner institutions to enable them as Shibboleth Resource Providers, and to disseminate learning in this area to the EPrints2 community.

A longer-term benefit of the project to participants was the creation at each site of a fully functional Shibboleth IdP, enabling all students and staff at all seven partner institutions to use the Shibboleth Identity Provider service for access to any Shibboleth-enabled resources within the Eduserv and SDSS Federations.

ShibboLEAP ran from 01 April 2005 to 28 April 2006. For more information, see the project web site at <http://www.angel.ac.uk/ShibboLEAP>.

#### **1.2. Sherpa-LEAP**

SHERPA-LEAP (London Eprints Access Project) began in April 2004, funded by the University of London Vice-Chancellor's Development Fund. In its first phase, SHERPA-LEAP developed open access eprint repositories for seven University of London institutions. The Project was subsequently awarded funding for a second phase, which began in February 2006; in the second phase, all University of London institutions will be invited into membership of the LEAP Consortium, and will be supported in developing institutional e-prints repositories. There are currently 10 SHERPA-LEAP repositories.

An important part of the work of SHERPA-LEAP is to engage with academics and researchers in identifying new models for the dissemination of research outputs. SHERPA-LEAP organises Conferences and publicises developments in the Scholarly Communications process.

SHERPA-LEAP is led by UCL, which also hosts 9 of the LEAP repositories.

For more information about SHERPA-LEAP, see <http://www.sherpa-leap.ac.uk>.

## **2. Organisational context**

Founded in 1826, UCL is London's leading multi-faculty University, and one of the most consistently highly-ranked research institutions in the UK after Oxford and Cambridge. The Government's 2001 Research Assessment Exercise awarded top marks of 5 or 5\* to 58 UCL Departments. UCL has a particular strength in clinical and pre-clinical studies: UCL has one of the largest Medical Schools in Europe, based on three campuses. All UCL medical libraries are currently joint libraries, serving both Higher Education and NHS users.

UCL research and teaching are carried out by more than 3,800 academic and research staff based in 72 academic Departments. In terms of student numbers, UCL has seen a steady growth during the last decade to 19,299 in the academic year 2005-06 (12,084 undergraduate and 7,215 postgraduate). Additionally, UCL employs over 1,000 administrative staff.

UCL, therefore, has a substantial number of identity holders, requiring access to a highly diverse portfolio of applications and resources. Local applications protected by some level of authentication include a VLE, Oracle Calendar diary software, the UCL intranet, various Unix services, and a number of other internal applications housed in different administrative Departments (a HR system, a Student Information System, a Finance System, etc). Access to a large proportion of UCL's on-line learning and research resources is administered by UCL Library Services, which currently makes available over 9000 electronic journals, around 200 indexing and/or full-text databases, and an increasing number of electronic books. Typically, these are authenticated by IP and/or by ATHENS, with a minority requiring additional, application-specific usernames and passwords. Where licences permit, access to members of the NHS, to members of learned societies affiliated to UCL, and to Library visitors, is given through dedicated "walk-in" terminals situated on Library premises. Authentication to these terminals is currently by Aleph (UCL's Library Management System) barcode and PIN.

UCL Library Services has recently made considerable progress towards single sign-on to its resources: ATHENS DA and ezproxy were implemented early in the 2005/6 session, and SSO has been incorporated into the MetaLib gateway, which is now being promoted to end-users as the preferred route to all the Library's e-resources. At UCL level, plans to introduce a common interface to many of the applications and resources described above through a UCL-wide Portal are in the early stages.

## **3. Technical environment: identity data and directory services**

### **3.1. Identity data**

The underlying data source for UCL directory services is the UCL Personal Index (UPI). The UPI is an Oracle-based index assigning a unique code to everyone who is, or ever has been, a *bona fide* member of UCL. The UPI collates data from UCL's Human Resources and Student Records systems, matching on name and date of birth so that, for example, if a student changes role and becomes a member of staff, he or she will retain the same UPI. (The UPI database, therefore, holds the previous and current UCL status of individuals and any history of department changes.)

Remedial work on this system was seen as a prerequisite to the successful installation of Shibboleth IdP. During ShibbolethLEAP, the system was re-engineered (NewUPI) to make it more efficient, to integrate it more seamlessly into the source databases, enabling clashes and matches to be flagged and resolved at the point of data entry, and to accommodate visiting and temporary staff at UCL. It is felt that the presence of good quality source data in UCL's directories, free from

duplicates and with accurate attributes, made the implementation of IdP significantly easier.

### **3.2. Directory Services**

Unix scripts build and maintain directory services from UPI data on a daily basis.

UCL has been running a directory service since 1989, when it took part in the X.500 directory pilot. The LDAP directory was a development from this service. UCL currently has two LDAP directories: one is a Windows 2000 Active Directory, which is used for authentication, and one is a public directory using OpenLDAP, containing telephone and email addresses.

The development of a third directory, using OpenLDAP, for authentication purposes only, is under consideration. This is because it is difficult to make schema changes to the Active Directory: using OpenLDAP will give more flexibility, particularly where applications require certain attributes as well as a valid userid and password. There are also privacy reasons for setting up a third directory: details of users who have elected to be ex-directory are omitted from the Active Directory, but could be included in the new OpenLDAP directory, as access to that data could be restricted to specific applications.

## **4. IdP Setup**

### **4.1. Components**

The IdP was set up on a dedicated server, which runs Slackware 9.0.0.

Web components: Apache 2.0.55 and Tomcat 5.5.

Directory service used: Active Directory.

Authentication is by mod\_auth\_ldap.

Little decision-making was involved in identifying this architecture: the existence of Active Directory and the work described above at 3.1 meant that these components could be selected with minimal discussion. However, it is expected that if the third, OpenLDAP directory described above at 3.2 is implemented, it will be used as the underlying directory for the UCL Shibb IdP, because of the greater configurability and flexibility in terms of attribute management of OpenLDAP over Active Directory.

There are plans to install a second Shibboleth IdP server for resilience purposes. This will be located in the UCL backup machine room, and Cisco load-balancing facilities will be used to make the two machines part of a farm with a single virtual IP address.

### **4.2. Certificates**

For the initial development, a certificate was purchased from 'Instant SSL', from whom UCL purchases most of its certificates, and who are much cheaper and quicker than some other certificate suppliers.

A GlobalSign certificate is required for membership of the Pilot SDSS Federation, and is currently being purchased for UCL. However, the ability to use the existing certificate for SDSS membership would have been preferable.

### **4.3. Installation and configuration**

The process of installing and configuring the above components was not smooth. The documentation at <http://shibboleth.internet2.edu/> on both installation and configuration was found to be unclear and poorly-structured. UCL also lacked local expertise in working with particular components, such as Tomcat. For these reasons,

the UCL Team relied heavily on the support of the Project Team at LSE (for which it is grateful). The process of IdP setup, therefore, was found to be somewhat drawn-out. However, no major departures from the architecture outlined above were necessary.

UCL IdP configuration files (idp.xml and resolver.xml) are appended to this document (see Appendices A and B respectively). The password used to access LDAP has been removed.

### **4.3. Resources required for IdP installation**

#### **4.3.1. Training / support requirements**

As noted above, UCL required intermittent support from the LSE Project Team, on matters such as the technicalities of Tomcat installation, clarification on attributes to be released, etc. Additionally, UCL's Technical Officer attended the 2-day MATU Course "*Deploying Shibboleth: v1.3 IdP*" (see <http://www.matu.ac.uk/uploaded-pdf/Deploying-Shibboleth-v1.3-IdP-Course-Outline.pdf>), which was found to be valuable.

#### **4.3.2. Time**

The initial ShibboLEAP project estimate of 0.4 FTE of a technical post over 12 months is considered to have been realistic. At UCL, this included work on re-engineering UCL's underlying person data, training and general learning around Shibboleth, internal briefing and communication, and project commitments, as well as the tasks directly associated with the implementation of Shibboleth IdP. UCL also configured an EPrints2 test server, mirroring the SHERPA-LEAP production server, for the purposes of developing and testing a Shibboleth authentication module for EPrints2. (This server was maintained until the decision was taken by the Project Team to use a local installation of EPrints2 for development.)

## **5. Dissemination and coordination, internal**

### **5.1 Institutional level**

The Project Coordinator was responsible for raising awareness of Shibboleth at UCL, particularly for ensuring engagement at appropriate levels of seniority with the national transition from ATHENS to Shibboleth.

UCL does not have a converged library and IT service. The regular route through which UCL Library Services discusses strategic priorities which require the support of UCL's Information Systems department is a standing Liaison Meeting between senior managers from the two departments. The Project Coordinator attended a meeting of this Group in order to raise strategic awareness of ShibboLEAP and Shibboleth, to explain the differences between Shibboleth and ATHENS DA (then only recently implemented at UCL) and to highlight the rationale and proposed timescales for the JISC's decision to move away from ATHENS.

Shibboleth is now a standing agenda item for this Meeting.

The text of a preliminary briefing note prepared for the Meeting (parts of which are understandably slightly out of date) follows:

**Internal briefing note prepared for UCL Information Systems / UCL Library Services joint senior managers' meeting, November 2005**

**Shibboleth, ShibboLEAP and ATHENS**

**Shibboleth**

Shibboleth is an access management architecture developed by the Internet2 Middleware Group. It uses open standards (eg SAML) to enable organisations to build single sign-on environments. Shibboleth technology manages the exchange of information between an organisation (the Identity Provider, or IdP) and a resource owner (the Resource Provider). The Identity Provider authenticates a user and passes attribute information about the user to the Resource Provider; the Resource Provider then decides whether or not to authorise access to the resource. Shibboleth protocols ensure that information is securely exchanged, and that the identity of the user remains private. Resource Providers may belong to one or more Federations, which are groups of organisations agreeing to a common set of policies for exchanging information about users and resources.

Conceptually, this is very similar to ATHENS DA. However, Shibboleth has been chosen as the next generation access management system for the JISC community. There are several underlying reasons for this.

Firstly, take-up of ATHENS outside the UK has been limited, meaning that resource suppliers have to pay significant sums of money to licence Athens for a relatively limited marketplace. Shibboleth is becoming an international standard: the US, Australia, and several European countries already have national programmes for Shibboleth adoption. Consolidation around a single global standard will reduce supplier costs, and reduce administrative complexity for customers like libraries.

Secondly, as well as supporting access to third-party resources, Shibboleth provides the flexibility to enable three other key scenarios to be supported in a uniform way:

- i) Access to internal resources, including administrative systems where role-based authorisation may be particularly important.
- ii) Inter-institutional resource sharing, eg the sharing of e-learning resources across a consortium.
- iii) Inter-institutional, dynamic research collaborations - the "virtual organisation".

Other benefits of Shibboleth are that it supports very sensitive role-based authorisation - in theory, this is limited only by the depth of detail of the organisation's own attribute store - and that it is extensible to support "new" methods of authentication, such as smart cards and biometrics.

**ShibboLEAP**

The JISC has funded 11 "Early Adopter" projects, each exploring Shibboleth implementations in various contexts, in order to build up the portfolio of Shibboleth experience and documentation within the community. UCL is participating in ShibboLEAP, the largest Early Adopters project, in which the 7 SHERPA-LEAP partners will each implement Shibboleth-based access management for their institutional repositories by April 2006. The lasting benefit of the project will be that 6 institutions, including UCL, will be newly-enabled as Shibboleth Identity Providers, and therefore prepared for the

move away from ATHENS. (LSE, which is leading ShibboLEAP, is already Shib-IdP enabled.) UCL's IdP is being configured by Adrian Barker, and successful UCL Shibboleth authentication has already been demonstrated.

### **ATHENS to Shibboleth: timescales and progress**

The JISC's current contract with EduserV to administer ATHENS ends in July 2006. This is renewable to July 2008, which is the latest end date for the contract. ATHENS as we know it will cease to be funded thereafter. Between now and July 2008 there will be a period of parallel operation, while Shibboleth becomes established.

Alongside Early Adopter support and related initiatives, transitional services funded by the JISC include an ATHENS-Shibboleth Gateway, which will enable Shibboleth adopters to access ATHENS-protected resources. LSE has implemented the ATHENS-Shibboleth Gateway, albeit with some teething troubles. The JISC-funded services hosted by Edina and Mimas are already Shibboleth-compliant, and may be used as targets for testing; and a full list of Shibboleth-compliant resources relevant to the UK community is in preparation. A pilot federation - SDSS, hosted by EDINA - has been established, and plans for a UK-wide federation are under way. Assuming that the technical issues uncovered by LSE are swiftly resolved, implementation of the ATHENS-Shibboleth Gateway at UCL warrants further consideration: if successful, it would certainly help to ease the transition to Shibboleth access management in 2008.

### **5.2 Other internal dissemination and consultation activity**

- Technical briefings to relevant colleagues given by Technical Officer
- Regular discussion between the Project Coordinator and UCL Library Services' Group Manager for IT Services throughout the project, and afterwards
- 1:1 briefings of key staff (the Ejournal Administrator, members of the IT Services Team) on an ad hoc basis by the Project Coordinator
- Shibboleth covered by Project Coordinator as part of Current Awareness talk open to all Library Services staff

### **6. Outstanding issues and future plans**

An application for a GlobalSign certificate is in progress, and registration with the SDSS Federation is in hand. The UCL Project Team will jointly see that this is carried through, albeit after the completion of ShibboLEAP.

A second IdP server is to be installed (see 4.2).

Experimentation with OpenLDAP continues; if successful, migration of the IdP from Active Directory to OpenLDAP will follow (see 4.2).

It is expected that the Athens-Shibboleth Gateway will be implemented some time after September 2006, when the Gateway becomes available to the UK Access Management Federation. Resources will then be migrated away from ATHENS DA one at a time. JORUM has been identified as an early candidate for migration to Shibboleth IdP: unlike UCL's other ATHENS-authenticated resources, JORUM is licensed for use only by UCL staff, which will enable a test of IdP attribute release to a relatively fine level of granularity. The precise timeframe for Gateway implementation will be determined by the IS/LS Liaison Meetings (see 5.1).

## Appendix A: UCL IdP Configuration - idp.xml and resolver.xml

### A.1. idp.xml

<!-- Shibboleth Identity Provider configuration -->

```
<IdPConfig
  xmlns="urn:mace:shibboleth:idp:config:1.0"
  xmlns:cred="urn:mace:shibboleth:credentials:1.0"
  xmlns:name="urn:mace:shibboleth:namemapper:1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:idp:config:1.0 ../schemas/shibboleth-
idpconfig-1.0.xsd"
  AAUrl="https://shib-dev.ucl.ac.uk:8443/shibboleth-idp/AA"
  resolverConfig="file:/usr/local/shibboleth-idp/etc/resolver.xml"
  defaultRelyingParty="urn:mace:eduserv.org.uk:athens:federation:uk"
  providerId="https://shib-dev.ucl.ac.uk/shibboleth">
```

<!-- This section contains configuration options that apply only to a site or group of sites

The signingCredential attribute value here needs to match the name of some credential defined

below -->

```
<RelyingParty name="urn:mace:ac.uk:sdss.ac.uk:federation:sdss"
  providerId="urn:mace:ac.uk:sdss.ac.uk:provider:identity:ucl.ac.uk"
  signingCredential="inqueue_cred">
  <NameID nameMapping="shm"/>
</RelyingParty>
```

```
<RelyingParty name="urn:mace:eduserv.org.uk:athens:federation:uk"
  providerId="urn:mace:eduserv.org.uk:athens:provider:ucl.ac.uk"
  signingCredential="inqueue_cred">
<NameID nameMapping="shm"/>
</RelyingParty>
```

```
<RelyingParty name="https://lse.ac.uk/shibboleth/federation/1"
  providerId="https://ucl.ac.uk/shibboleth/origin/1"
  signingCredential="inqueue_cred">
<NameID nameMapping="shm"/>
</RelyingParty>
```

<!-- Change only path here if necessary -->

```
<ReleasePolicyEngine>
  <ArpRepository
implementation="edu.internet2.middleware.shibboleth.aa.arp.provider.FileSystemArp
Repository">
```

```
  <Path>file:/usr/local/shibboleth-idp/etc/arps/</Path>
```

```
  </ArpRepository>
```

```
</ReleasePolicyEngine>
```

<!-- Logging Configuration

The defaults work fine in this section, but it is sometimes helpful to use "DEBUG" as the level for

the <ErrorLog/> when trying to diagnose problems -->

```
<Logging>
```

```

        <ErrorLog level="WARN" location="file:/usr/local/shibboleth-idp/logs/shib-error.log" />
        <TransactionLog level="INFO" location="file:/usr/local/shibboleth-idp/logs/shib-access.log" />
    </Logging>

    <!-- This configuration section determines how Shibboleth maps between SAML
    Subjects and local principals.
    Do not change! -->
    <NameMapping
        xmlns="urn:mace:shibboleth:namemapper:1.0"
        id="shm"
        format="urn:mace:shibboleth:1.0:nameIdentifier"
        type="SharedMemoryShibHandle"
        handleTTL="28800"/>

    <!-- Determines how SAML artifacts are stored and retrieved
    Do not change! -->
    <ArtifactMapper
implementation="edu.internet2.middleware.shibboleth.artifact.provider.MemoryArtifactMapper" />

    <!-- This configuration section determines the keys/certs to be used when
    signing SAML assertions -->
    <!-- The credentials listed here are used when referenced within
    <RelyingParty/> elements above -->
    <!-- Change only if key/certificate locations are changed -->
    <Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
        <FileResolver Id="inqueue_cred">
            <Key format="PEM">
                <Path>file:/usr/local/apache2/conf/ssl.key/shib-dev.key</Path>
            </Key>
            <Certificate format="PEM">
                <Path>file:/usr/local/apache2/conf/ssl.crt/shib-dev\_ucl\_ac\_uk.crt</Path>
            <!-- Is the CAPath needed ??
                <CAPath>file:/usr/local/apache2/conf/ssl.crt/secureroots.crt</CAPath>
            </Path>
            -->

            </Certificate>
        </FileResolver>
    </Credentials>

    <!-- Protocol handlers specify what type of requests the IdP can respond
    to. The default set listed here should work
    for most configurations. Do not change. -->
    <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.ShibbolethV1SSOHandler">
        <Location>https://\[^\:\]+\:\(443|80\)?/shibboleth-idp/SSO</Location> <!--
    regex works when using default protocol ports -->

```

```

        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.SAMLv1_Attribute
QueryHandler">
            <Location>.+:8443/shibboleth-idp/AA</Location>
        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.SAMLv1_1Artifact
QueryHandler">
            <Location>.+:8443/shibboleth-idp/Artifact</Location>
        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.Shibboleth_Status
Handler">
            <Location>https://\[^:\]+\(:443\)?/shibboleth-idp/Status</Location>
        </ProtocolHandler>

```

<!-- This section configures the loading of SAML2 metadata, which contains information about system entities and how to authenticate them. The metadatatool utility can be used to keep federation metadata files in synch.

Metadata can also be placed directly within this these elements. -->

```

        <MetadataProvider
type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMetadata"
uri="file:/usr/local/shibboleth-idp/etc/shibboleap.xml"/>
</IdPConfig>

```

## A.2. resolver.xml

*Note: password required for access to LDAP has been removed*

```

<AttributeResolver xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:mace:shibboleth:resolver:1.0"
xsi:schemaLocation="urn:mace:shibboleth:resolver:1.0 shibboleth-resolver-1.0.xsd">

```

<!--

```

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonEntitlement">

```

```

        <DataConnectorDependency requires="echo"/>

```

```

    </SimpleAttributeDefinition>

```

```

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonAffiliation">

```

```

        <DataConnectorDependency requires="echo"/>

```

```

    </SimpleAttributeDefinition>

```

-->

<!-- To use these attributes, you should change the smartScope value to match your site's domain name. -->

<!--

```

    <SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation" smartScope="ucl.ac.uk">

```

```

        <AttributeDependency requires="urn:mace:dir:attribute-
def:eduPersonAffiliation"/>

```

```

    </SimpleAttributeDefinition>

```

```

</SimpleAttributeDefinition>

<SimpleAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonPrincipalName" smartScope="ucl.ac.uk">
  <DataConnectorDependency requires="echo"/>
</SimpleAttributeDefinition>

-->

<!-- UCL LDAP -->
<RegexAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonPrincipalName"
  sourceName="cn"
  regex="$" replacement="@ucl.ac.uk"
  ignoreCase="true" partialMatch="true">
  <DataConnectorDependency requires="directory"/>
</RegexAttributeDefinition>

<RegexAttributeDefinition id="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation"
  sourceName="description"
  regex="staff|p|g|u|g" replacement="member"
  ignoreCase="true" partialMatch="true">
  <DataConnectorDependency requires="directory"/>
</RegexAttributeDefinition>

<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:mail" >
  <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>

<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:ou"
  sourceName="department">
  <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>

<!-- Example persistent id attribute. Since this configuration is permanent, some
thought is required before
  deploying in production. Consider replacing this with a database-backed
mechanism of some sort. -->

  <SAML2PersistentID id="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
sourceName="employee_ID">
  <DataConnectorDependency requires="directory"/>
  <Salt keyStorePath="file:///usr/local/shibboleth-idp/etc/persistent.iks"
keyStoreKeyAlias="handleKey" keyStorePassword="shibhs"
keyStoreKeyPassword="shibhs"/>
  </SAML2PersistentID>

  <!-- Deprecated persistent id example, use only with SPs that are already
relying on your values. -->
  <!--
  <PersistentIDAttributeDefinition id="urn:mace:dir:attribute-

```

```

def:eduPersonTargetedID" scope="shibdev.edu" sourceName="guid">
    <DataConnectorDependency requires="echo"/>
    <Salt keyStorePath="file:///usr/local/shibboleth-idp/etc/persistent.jks"
keyStoreKeyAlias="handleKey" keyStorePassword="shibhs"
keyStoreKeyPassword="shibhs"/>
</PersistentIDAttributeDefinition>
-->

    <CustomDataConnector id="echo"
class="edu.internet2.middleware.shibboleth.aa.attrresolv.provider.SampleConnector"
/>

    <JNDIDirectoryDataConnector id="directory">
        <Search filter="cn=%PRINCIPAL%">
            <Controls searchScope="SUBTREE_SCOPE"
returningObjects="false" />
        </Search>
        <Property name="java.naming.factory.initial"
value="com.sun.jndi ldap.LdapCtxFactory" />
        <Property name="java.naming.provider.url" value="ldap://uclusers-
dc1.uclusers.ucl.ac.uk/dc=uclusers,dc=ucl,dc=ac,dc=uk" />
        <Property name="java.naming.security.principal"
value="cn=*****,ou=System Users,dc=uclusers,dc=ucl,dc=ac,dc=uk" />
        <Property name="java.naming.security.credentials" value="*****" />
    </JNDIDirectoryDataConnector>

</AttributeResolver>

```