



# Active Directory & Shibboleth

**Nigel Bruce**

IT Manager

ISS, University of Leeds

[N.Bruce@leeds.ac.uk](mailto:N.Bruce@leeds.ac.uk)





## Active Directory

- Moved to AD from NDS & eDirectory 4 years ago.
- AD contains 32,500 students and 7,500 staff accounts.
- Used to authenticate access to PCs and to file & print services which are predominantly Windows 2003/SAN based.
- 95% of staff use Exchange 2003.
- SMS 2003 is used for application deployment to staff & students.
- About 14,000 PCs on campus. 9000 PCs currently in AD. Rest to follow.



## Active Directory

- Lynchpin of University's Simplified and Single SO strategy.
- Currently many non-Microsoft systems now use AD for authN/AuthZ.
  - Student Portal – SCT Luminis
  - Banner Student Information System – self-service for students
  - On-line module enrolment
  - Wireless LAN – via Blue Socket
  - VPN – Cisco VPN Concentrator
  - Student IMAP mail service – University of Washington IMAP Server on Solaris with IMP Web Interface
  - University Library Catalogue – Innopac
  - Solaris w/s clusters
  - Numerous websites via LDAP
- In future
  - On-line Registration System – August 1<sup>st</sup> 2006
  - SAP Finance & HR - via SAP Enterprise Portal
  - Banner Student Information System – for staff
  - VLE – Bodington (from August 2006)
  - Athens resources via Athens-Shibboleth Gateway (from September 2006)



## LURCIS

- Active Directory is increasingly vital to the University's entire IT & IS infrastructure.
- Accounts in AD generated from our meta-directory, LURCIS, via LDAP.
- Leeds **U**niversity **R**egistration & **C**ertificate **I**ssuing **S**ervice.
- SQL 2000 database.
- LURCIS populated from SAP HR and Banner SIMS.
- LURCIS contains more information on staff and students than AD.
- AD was the obvious means of authentication we would use from our IdP.
- Didn't want to extend the schema of our AD with the EduPerson schema class.
- Decision made to use LURCIS as the Attribute Store rather than AD.
- Two main reasons – to avoid unnecessary risk & increase flexibility.



### University of Leeds IdP

- We currently use EduserV's AthensIM implementation of Shibboleth on our IdP.
- Runs on a Windows 2003 server under Tomcat.
- We use LDAP to authenticate users to the Handle Service. Ruled out Windows Integrated Authentication.
- Intend to move to Internet2 release when version 2.0 comes out.
- We developed Custom Attribute Processors within the IdP which sends whatever information the Service Provider requires in whatever format is needed. e.g. access to Athens resources can be denied or allowed through a flag set in LURCIS.



## General Points

- AD not necessarily the right place to store large amounts of data on your users , e.g. module enrolment.
- If you have to use AD then AD Application Mode (ADAM) might be more appropriate, esp. if you have to synchronise your AD across slow network links.
- Relational DBMS such as SQL Server or Oracle are more flexible tools. Changes made to DBs carry less risk.
- Shibboleth doesn't dictate how authentication is done nor where attributes are retrieved from so long as they are expressed 'correctly'.
- Be pragmatic! Do what's right for your institution. Depends on where you're starting from, skills available to you and the context of where you're heading.



# Questions?

**Nigel Bruce**

IT Manager

ISS, University of Leeds

[N.Bruce@leeds.ac.uk](mailto:N.Bruce@leeds.ac.uk)

