“The Road Ahead”

Jon Dowland, Cal Racey,
University of Newcastle upon Tyne

Shibboleth

Then said they unto him, Say now **Shibboleth**: and he said Sibboleth: for he could not frame to pronounce it right. Then they took him, and slew him at the passages of Jordan: and there fell at that time of the Ephraimites forty and two thousand.

Judges 12:5-7

Shibboleth

"Shibboleth, is a bit like the duck which moves serenely through the water, but is paddling furiously beneath the surface."

- Derek Morrison, the Auricle

Overview

- Who are we?
- Technical issues
- Managerial issues
- Future Developments

Who are we?

- "**I**nter-institutional **A**uthorisation **M**anagement to **S**upport **e**Learning with reference to **C**linical **T**eaching"

Inter-institutional

- Newcastle
  - FMSC
  - ISS
- Durham
  - ISS

Who are we?

- Core-middleware project since ~July ’04
- Relationships with:
  - SAPIR (early adopters)
  - EPICS (distributed e-learning)

Technical Issues

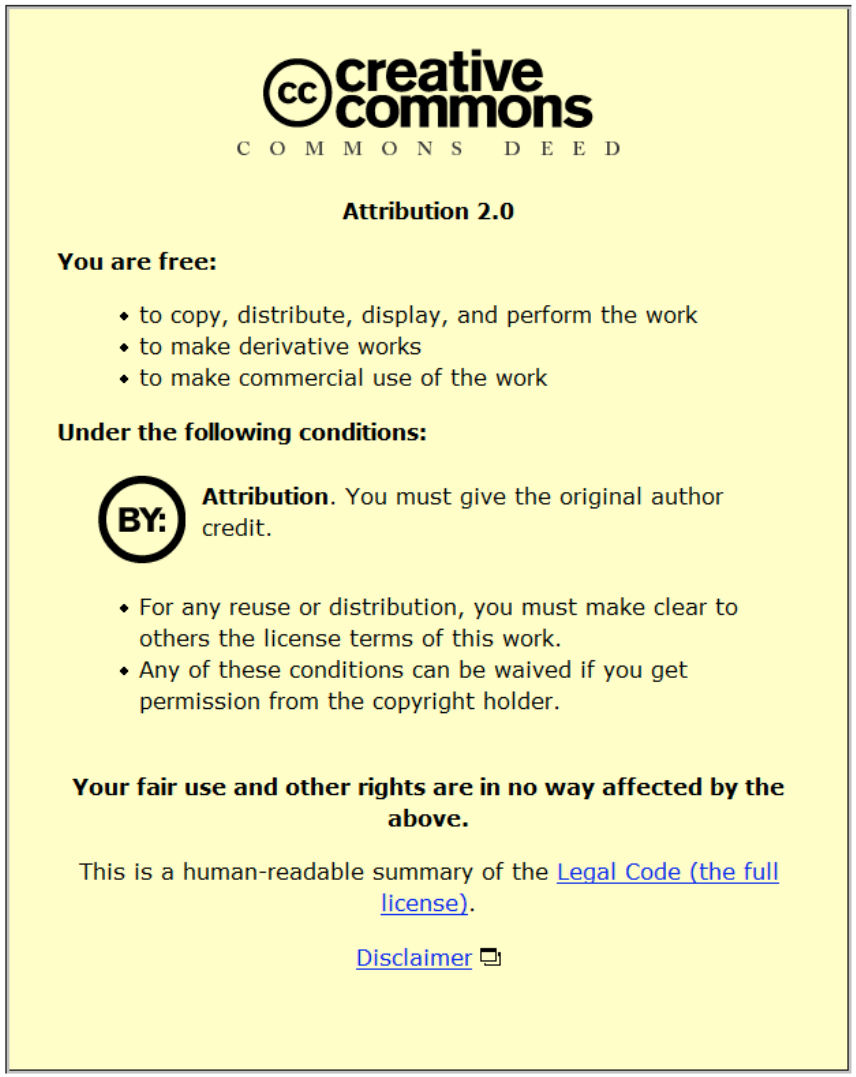
First experiences

- Technical angle / software installation
- Hard.

Technical documents

- From first experiences
  - Installing Shibboleth on Redhat AS 3.0 and using pubcookie
  - Installing Pubcookie on Redhat AS 3.0 and authenticating against Windows Active Directory

Creative Commons

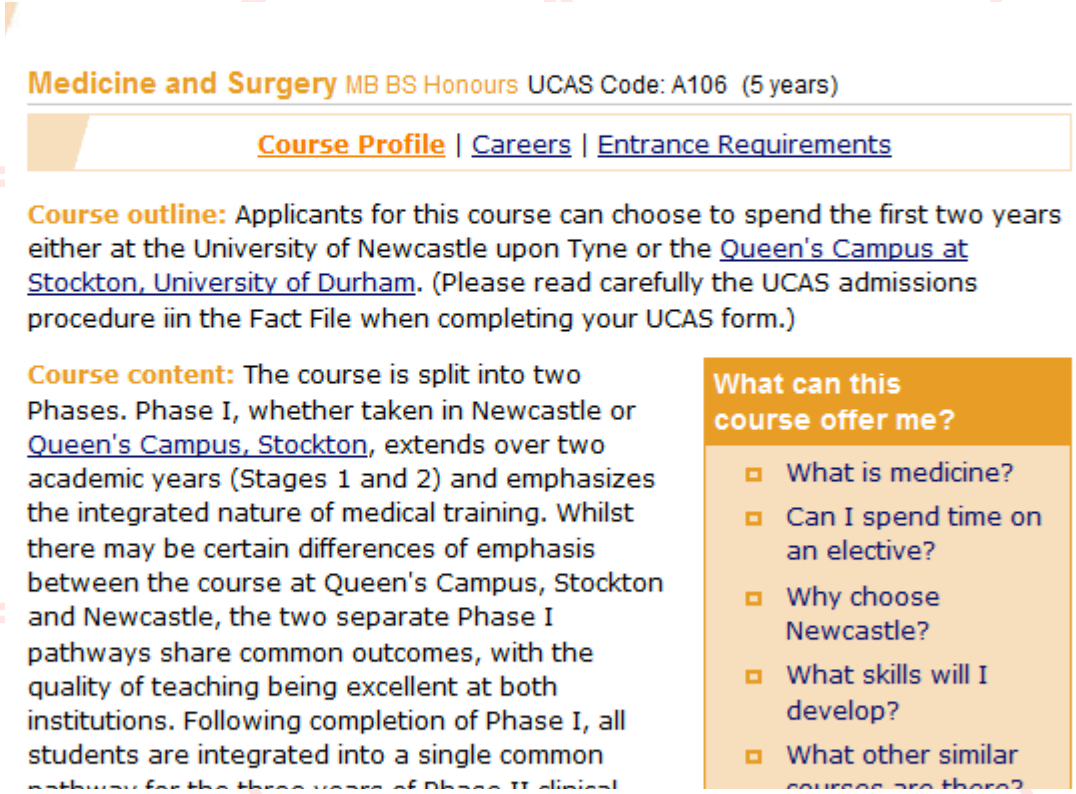


Authorisation, **C**linical **T**eaching

- a proverbial goldmine of privacy and confidentiality issues
- Involvement of Newcastle FMSC

Authorisation, Clinical Teaching

- Shared students: Durham/Newcastle



Medicine and Surgery MB BS Honours UCAS Code: A106 (5 years)

Course Profile | Careers | Entrance Requirements

Course outline: Applicants for this course can choose to spend the first two years either at the University of Newcastle upon Tyne or the Queen's Campus at Stockton, University of Durham. (Please read carefully the UCAS admissions procedure iin the Fact File when completing your UCAS form.)

Course content: The course is split into two Phases. Phase I, whether taken in Newcastle or Queen's Campus, Stockton, extends over two academic years (Stages 1 and 2) and emphasizes the integrated nature of medical training. Whilst there may be certain differences of emphasis between the course at Queen's Campus, Stockton and Newcastle, the two separate Phase I pathways share common outcomes, with the quality of teaching being excellent at both institutions. Following completion of Phase I, all students are integrated into a single common

What can this course offer me?

- What is medicine?
- Can I spend time on an elective?
- Why choose Newcastle?
- What skills will I develop?
- What other similar

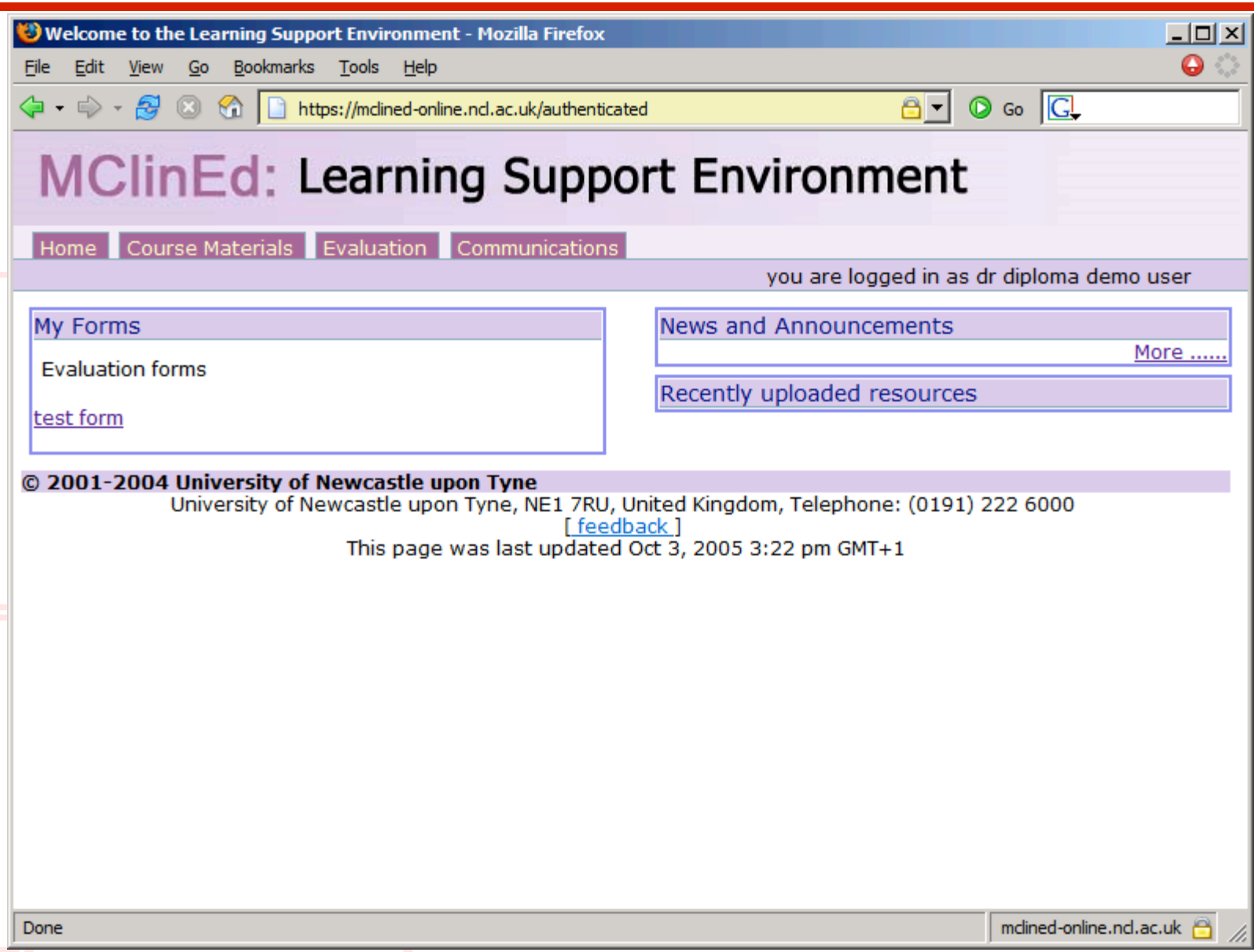
Authorisation, **C**linical **T**eaching

- In-house medical-oriented virtual learning environment (VLE)
- “Shibbolized”

MClinEd

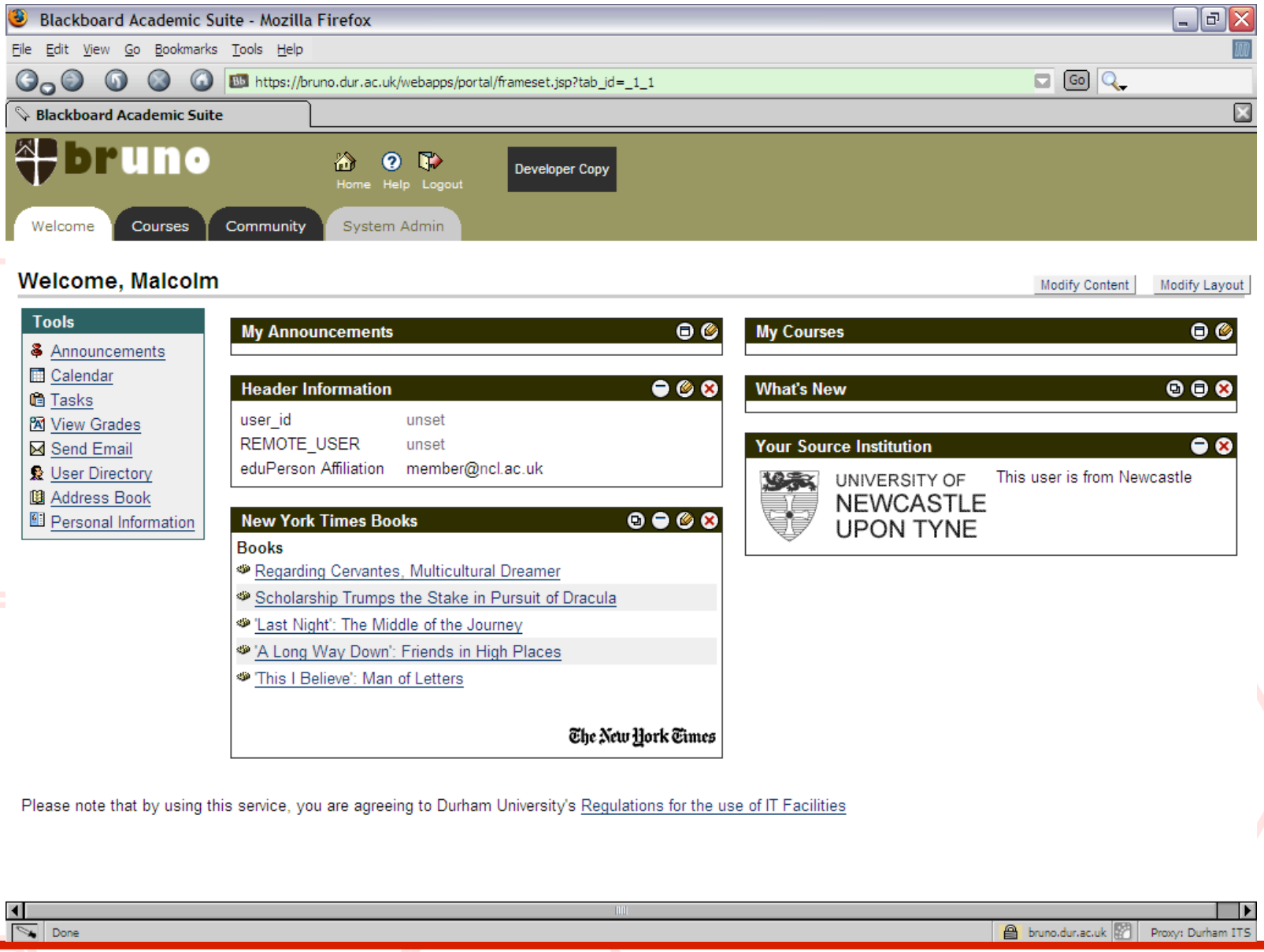
- Medical School's VLE
- Zope
- Shibboleth + Apache

- Local IdP
- Connected with Fast CGI
  - deprecated


Welcome to the Learning Support Environment - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://mclined-online.ncl.ac.uk/authenticated
Go
MClinEd: Learning Support Environment
Home
Course Materials
Evaluation
Communications
you are logged in as dr diploma demo user
My Forms
Evaluation forms
test form
News and Announcements
More .....
Recently uploaded resources
© 2001-2004 University of Newcastle upon Tyne
University of Newcastle upon Tyne, NE1 7RU, United Kingdom, Telephone: (0191) 222 6000
[feedback]
This page was last updated Oct 3, 2005 3:22 pm GMT+1
Done
mclined-online.ncl.ac.uk

Blackboard VLE

- Durham's Blackboard VLE
- Shibbolized
  - used with local IdP


Blackboard Academic Suite - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://bruno.dur.ac.uk/webapps/portal/frameset.jsp?tab_id=_1_1
Blackboard Academic Suite
bruno
Home Help Logout
Developer Copy
Welcome Courses Community System Admin
Welcome, Malcolm
Modify Content Modify Layout
Tools
Announcements
Calendar
Tasks
View Grades
Send Email
User Directory
Address Book
Personal Information
My Announcements
Header Information
user_id unset
REMOTE_USER unset
eduPerson Affiliation member@ncl.ac.uk
New York Times Books
Books
Regarding Cervantes, Multicultural Dreamer
Scholarship Trumps the Stake in Pursuit of Dracula
'Last Night': The Middle of the Journey
'A Long Way Down': Friends in High Places
'This I Believe': Man of Letters
The New York Times
My Courses
What's New
Your Source Institution
UNIVERSITY OF NEWCASTLE UPON TYNE
This user is from Newcastle
Please note that by using this service, you are agreeing to Durham University's Regulations for the use of IT Facilities
Done
bruno.dur.ac.uk
Proxy: Durham ITS

Technical Issues

Shibboleth Administration

Shibboleth administration

The process of setting up an attribute:

- Aggregation
- Release
- Acceptance

Complexity

```
 <SimpleAttributeDefinition id="urn:mace:dir:attribute-
    def:eduPersonEntitlement" sourceName="sdssentitlement"
    smartScope="ncl.ac.uk">

    <DataConnectorDependency requires="db6"/>
</SimpleAttributeDefinition>


<JDBCDataConnector id="db6"

    dbURL="jdbc:mysql://thing.ncl.ac.uk/OilDrum?user=thing&amp;password=thing"

    dbDriver="com.mysql.jdbc.Driver"
    maxActive="10"
    maxIdle="5">
 <Query>
SELECT course_code,
CASE course_code
WHEN 'A101' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN 'A106' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN 'O106' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN '3019P' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN '3384P' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN '5826P' THEN 'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
ELSE 'none' END

as sdssentitlement FROM CMstudentdata WHERE loginid = ?</Query>
</JDBCDataConnector>
```

Complexity

ARP.xml

```
<Rule>
<Description>EMOL service at EDINA</Description>
   <Target>
      <Requester>
urn:mace:ac.uk:sdss.ac.uk:provider:service:emol.sdss
   .ac.uk
      </Requester>
   </Target>
<Attribute name="urn:mace:dir:attribute-
   def:eduPersonEntitlement">
   <Value release="permit">
urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.u
   k:restricted
   </Value>
</Attribute>
</Rule>
```

AAP.xml

```
<AttributeRule  Name="urn:mace:dir:attribute-
  def:eduPersonAffiliation" Header="Shib-EP-
  UnscopedAffiliation-edit" Alias="unscoped-
  affiliation">
  <AnySite>
     <Value Type="regexp">
          ^[M|m][E|e][M|m][B|b][E|e][R|r]$
     </Value>
  </AnySite>
</AttributeRule>
```

Complexity

- No tools to help the admin (yet)
- Editing verbose opaque xml files by hand
- Looking in verbose opaque log files
- Asking others to look in verbose opaque log files at their end
- Security gets in the way

- Magic is cool flexible but hard to grasp.

Technical Issues

Where to get help?

Technical help

- Us
  - http://iamsect.ncl.ac.uk/deliverables/
- Internet2 –
  - http://shibboleth.internet2.edu/guides/idp/
  - http://shibboleth.internet2.edu/guides/sp
  - https://authdev.it.ohio-state.edu/twiki/bin/view/Shibboleth/WebHome
- SDSS federation –
  - http://sdss.ac.uk/wiki/wiki.pl?SdssWiki

Managerial Issues

Complex Attributes

Complex attributes

- Use case
- Generation
- Problems
- Lessons learned

Complex attributes: Example

“Medic restrict”

- Accessing medical content at EMOL
- Subset of resources e.g. Autopsy content

Requires entitlement attribute:

edupersonEntitlement

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

Complex attributes: students

- “Relatively” easy for students-

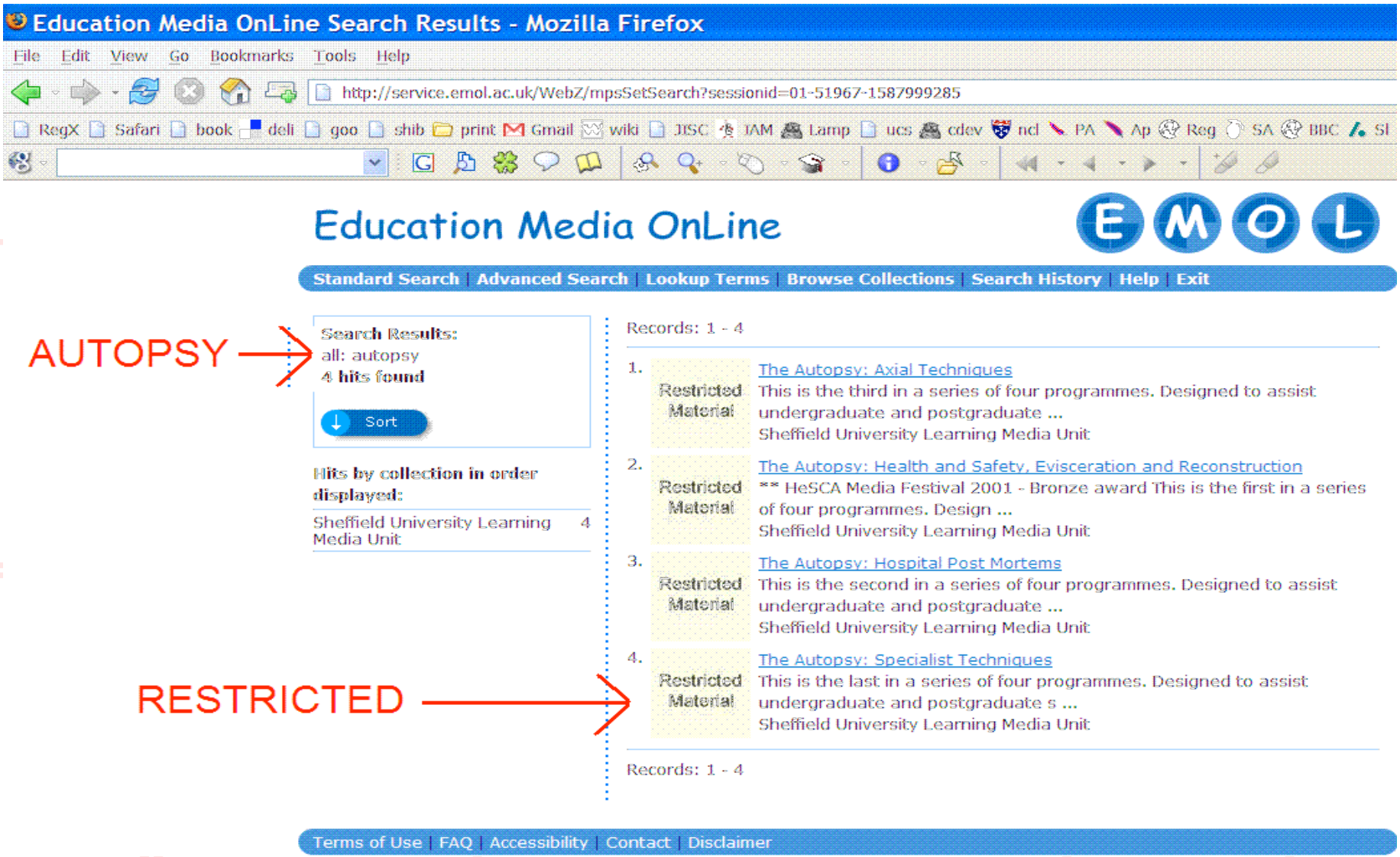
```
SimpleAttributeDefinition
    id="urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk“
sourceName="sdssentitlement“

SELECT course_code,
CASE course_code
WHEN 'A101' THEN
    'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
WHEN 'A106' THEN
    'urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted'
ELSE 'none' END
as sdssentitlement FROM CMstudentdata WHERE loginid = ?
```

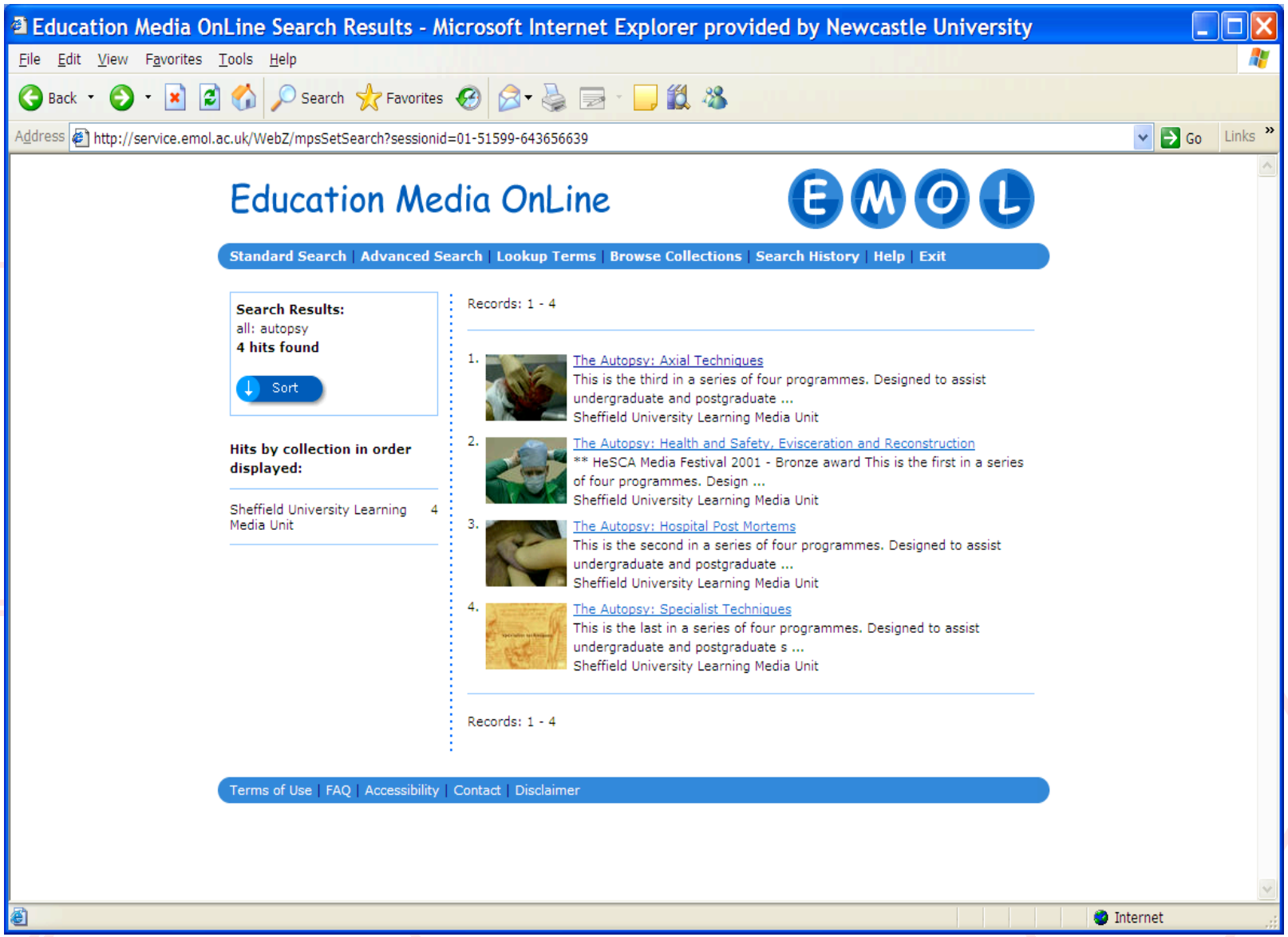
- Find out if student is on one of three medical courses

Complex attributes: Staff

- Staff, registered manually over years
- Pick their own usernames, own email address – most didn't use @ncl.ac.uk address
- No connection between Athens id and Newcastle id
- NHS staff have ncl usernames

Solution?


Education Media OnLine Search Results - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://service.emol.ac.uk/WebZ/mpsSetSearch?sessionid=01-51967-1587999285
Education Media OnLine
EMOL
Standard Search | Advanced Search | Lookup Terms | Browse Collections | Search History | Help | Exit
AUTOPSY
Search Results:
all: autopsy
4 hits found
Sort
Hits by collection in order displayed:
Sheffield University Learning Media Unit 4
Records: 1 - 4
1. Restricted Material
The Autopsy: Axial Techniques
This is the third in a series of four programmes. Designed to assist undergraduate and postgraduate ...
Sheffield University Learning Media Unit
2. Restricted Material
The Autopsy: Health and Safety, Evisceration and Reconstruction
** HeSCA Media Festival 2001 - Bronze award This is the first in a series of four programmes. Design ...
Sheffield University Learning Media Unit
3. Restricted Material
The Autopsy: Hospital Post Mortems
This is the second in a series of four programmes. Designed to assist undergraduate and postgraduate ...
Sheffield University Learning Media Unit
4. Restricted Material
The Autopsy: Specialist Techniques
This is the last in a series of four programmes. Designed to assist undergraduate and postgraduate s ...
Sheffield University Learning Media Unit
RESTRICTED
Records: 1 - 4
Terms of Use | FAQ | Accessibility | Contact | Disclaimer


Education Media OnLine Search Results - Microsoft Internet Explorer provided by Newcastle University
File Edit View Favorites Tools Help
Back Search Favorites
Address http://service.emol.ac.uk/WebZ/mpsSetSearch?sessionid=01-51599-643656639
Go Links
Education Media OnLine
EMOL
Standard Search | Advanced Search | Lookup Terms | Browse Collections | Search History | Help | Exit
Search Results:
all: autopsy
4 hits found
Sort
Hits by collection in order displayed:
Sheffield University Learning Media Unit 4
Records: 1 - 4
1. The Autopsy: Axial Techniques
This is the third in a series of four programmes. Designed to assist undergraduate and postgraduate ...
Sheffield University Learning Media Unit
2. The Autopsy: Health and Safety, Evisceration and Reconstruction
** HeSCA Media Festival 2001 - Bronze award This is the first in a series of four programmes. Design ...
Sheffield University Learning Media Unit
3. The Autopsy: Hospital Post Mortems
This is the second in a series of four programmes. Designed to assist undergraduate and postgraduate ...
Sheffield University Learning Media Unit
4. The Autopsy: Specialist Techniques
This is the last in a series of four programmes. Designed to assist undergraduate and postgraduate s ...
Sheffield University Learning Media Unit
Records: 1 - 4
Terms of Use | FAQ | Accessibility | Contact | Disclaimer
Internet

Lessons learned

- Complex attributes are hard
- All solutions assume you have good information to hand
- Medical user base is extremely complicated

Need better information:

- Chicken and egg
  - No one will put system in place to record attribute until needed
  - No one will require an attribute unless already stored

Solution

Need for a information reorganisation

Registration and expiry to all different systems is unmanageable:

Management system (ERPs) - SAP

VLEs- blackboard, zope, moodle, Ness

Library – metalib, reading lists, Athens

Mail, Active directory, network,

Proposal 1 central repository feeding many consumers:

Potential Tools to help

- Nexus and Open Metadirectory(OM)
  - tools for provisioning user accounts into different systems,
  -Potential to get good attributes.

- Grouper: aggregates existing group info
  -relies on having that info
- Signet: tool for managing and assigning privileges

Managerial Issues

Supporting users

Support Issues

Testing

- The need for testing
- How to test
- Access Problems:

  -why they will happen
  -what they look like
  -what should they look like

The need for testing

The fantasy

Shibboleth relies on accurate easily locatable institutional information

The reality

Information stores are:

- dispersed,
- inaccessible,
- incomplete,
- out of sync,
- conflicting.

Attributes accuracy is “a best effort” not a certainty

Things will go wrong

Examples

EdupersonScoped Affiliation

- Ability to login should = ncl affiliation
  - NHS staff
  -101 edge cases

EdupersonEntitlement medic restrict

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

Identifying medics is hard,

There will be plenty of problems

The problem of testing

- How do you test access control setup for all the different user types?

- Test users are difficult to setup,
- In multiple attribute store scenario they have to be in all stores.
- some stores don’t understand “fake users”

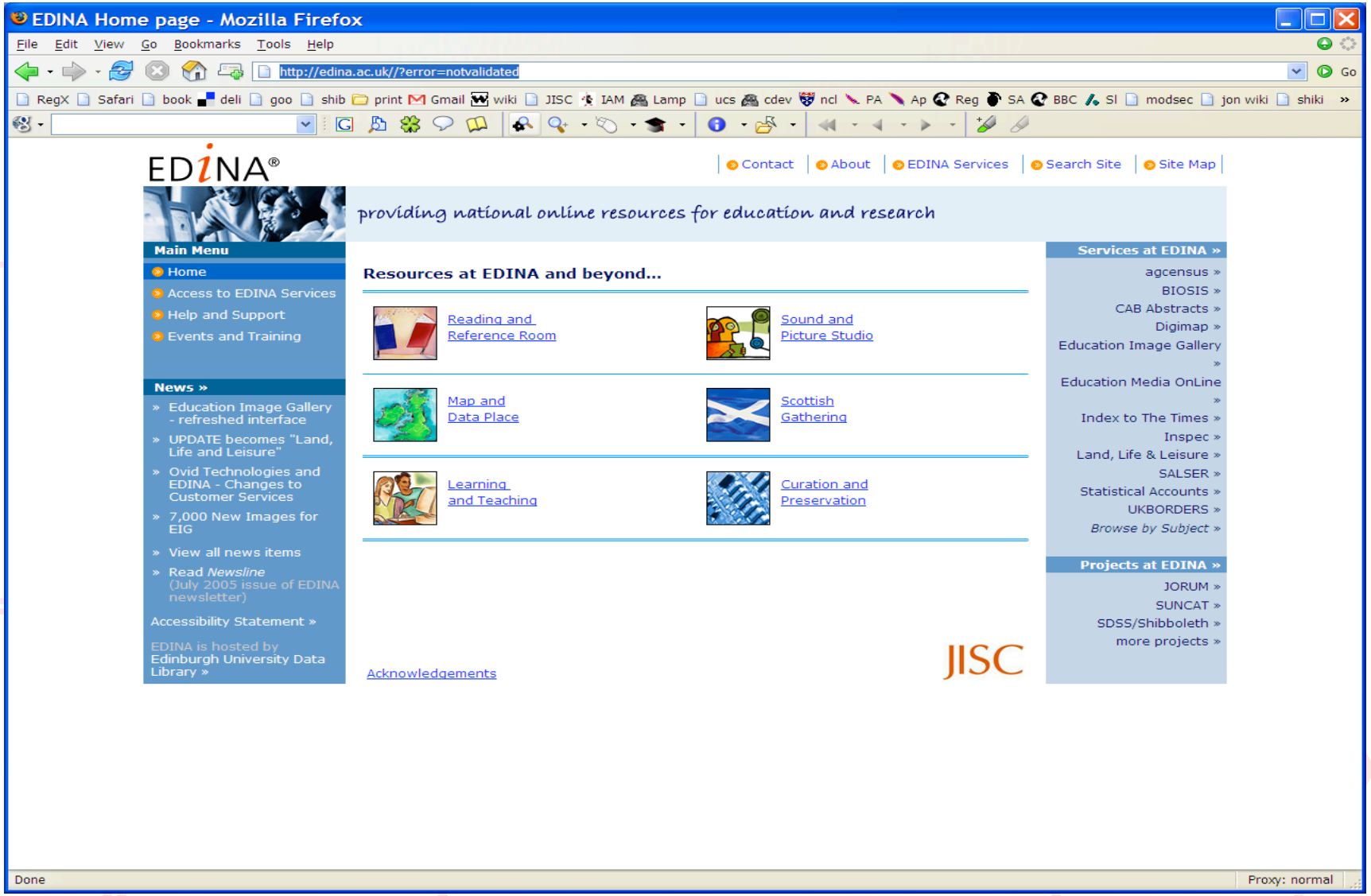
When things go wrong

- Middleware is invisible:
  - when it works
  - when it doesn't

  - users unaware of what success looks like, therefore unaware of failure
  -federated content means federated errors

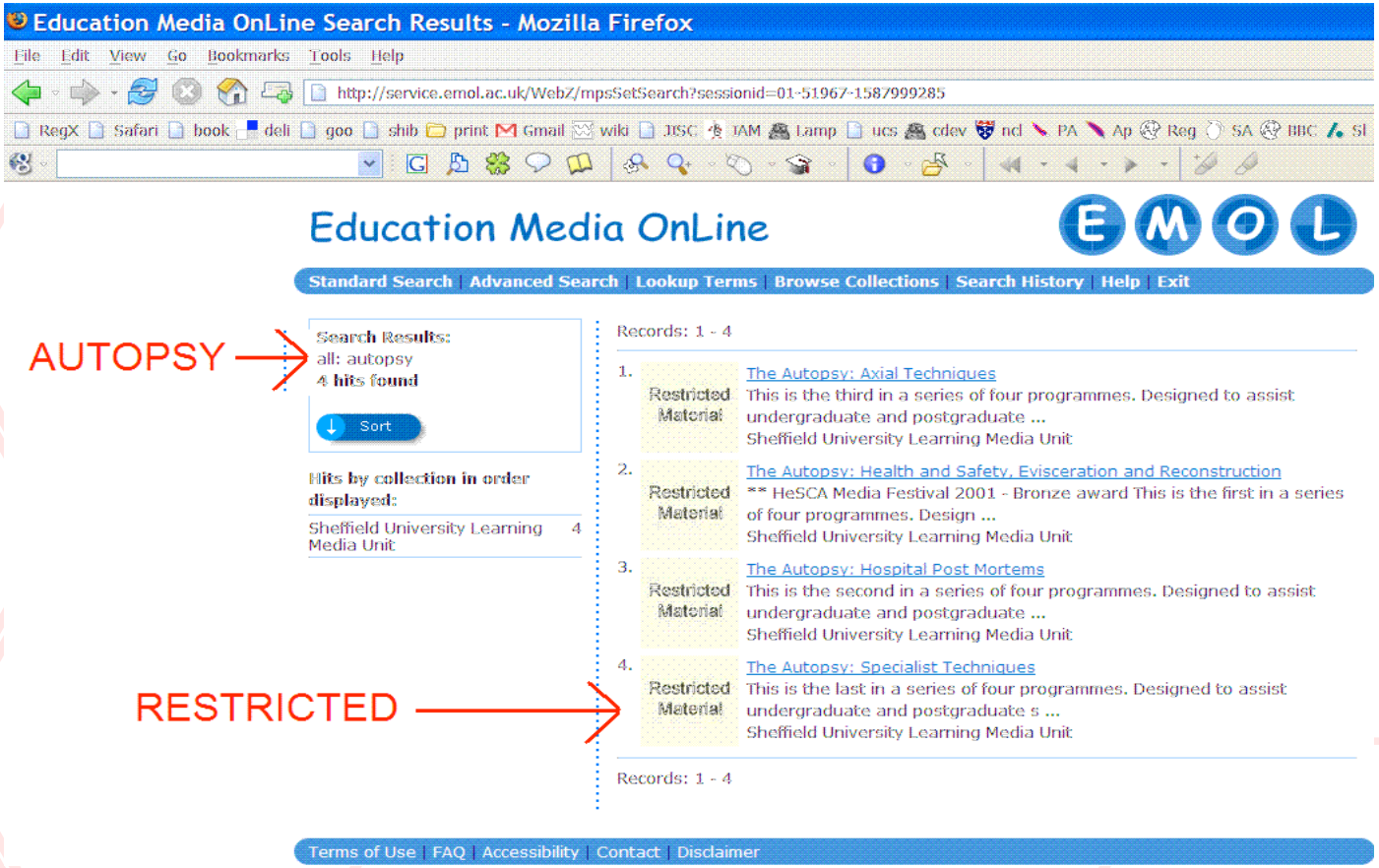
Similar to networking problems

Access to EMOL



Access without proper scopedAffiliation

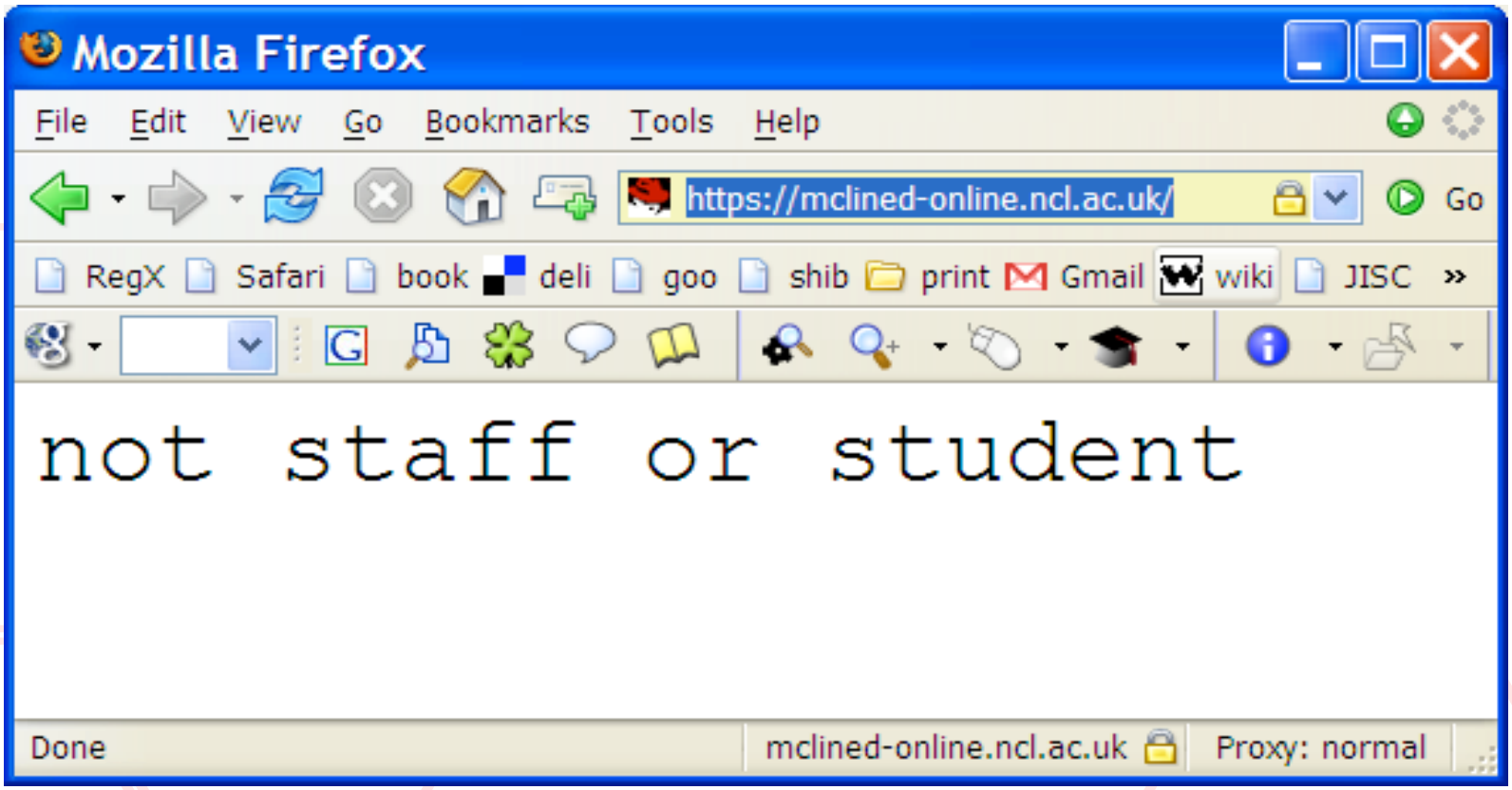
Access to EMOL



Access without medical entitlement

- Tells you something is wrong
- However no obvious route to rectify it

Local VLE



Access by non med school user

What improperly registered medics see

Managerial Issues

Legal Issues

Legal Issues

- Liability

- Initially assessed as “medium-severity, low probability” risk
- Could be a project in itself

Managerial Issues

Where to get help?

Managerial Documents

- Drafts up
  - Introduction to Shibboleth Federations
  - Practical access to electronic journals using Shibboleth
  - Attribute identification and storage for Shibboleth

- http://iamsect.ncl.ac.uk/deliverables/

Managerial help

- Us
  - http://iamsect.ncl.ac.uk/deliverables/
- JISC
  - http://www.jisc.ac.uk/uploaded_documents/CMRoadmap03_05.doc - *Connecting People to Resources*
- ?

Future developments

Standardisation

- OS Integration
  - `apt-get install shibboleth-service-provider`
  - **(or whatever)**
- Application support
- National federation

‘Odd ones out’ Identity Provider

- Industry/Academic/Clinical collaborations
  - Those without home institutions
  - Home institutions without Shibboleth

Conclusion

Optimism

There are problems, however:

- Once setup it just works (!)
- Robust
- Recipes easy
- Building tools should be easy
- It enables cool stuff

Questions