Inter-institutional Authorisation using Shibboleth: *Myths, Lies and the Truth*

Jon Dowland

iamsect project officer

University of Newcastle upon Tyne

Overview

- Definition and demonstration

- Current state of the art
- Shibboleth is…
- Who's doing what?

- Wrap-up
- Questions

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*

Live demonstration

Statement

Shibboleth is a Single Sign-On (SSO) solution

Statement

Shibboleth is a Single Sign-On (SSO) solution

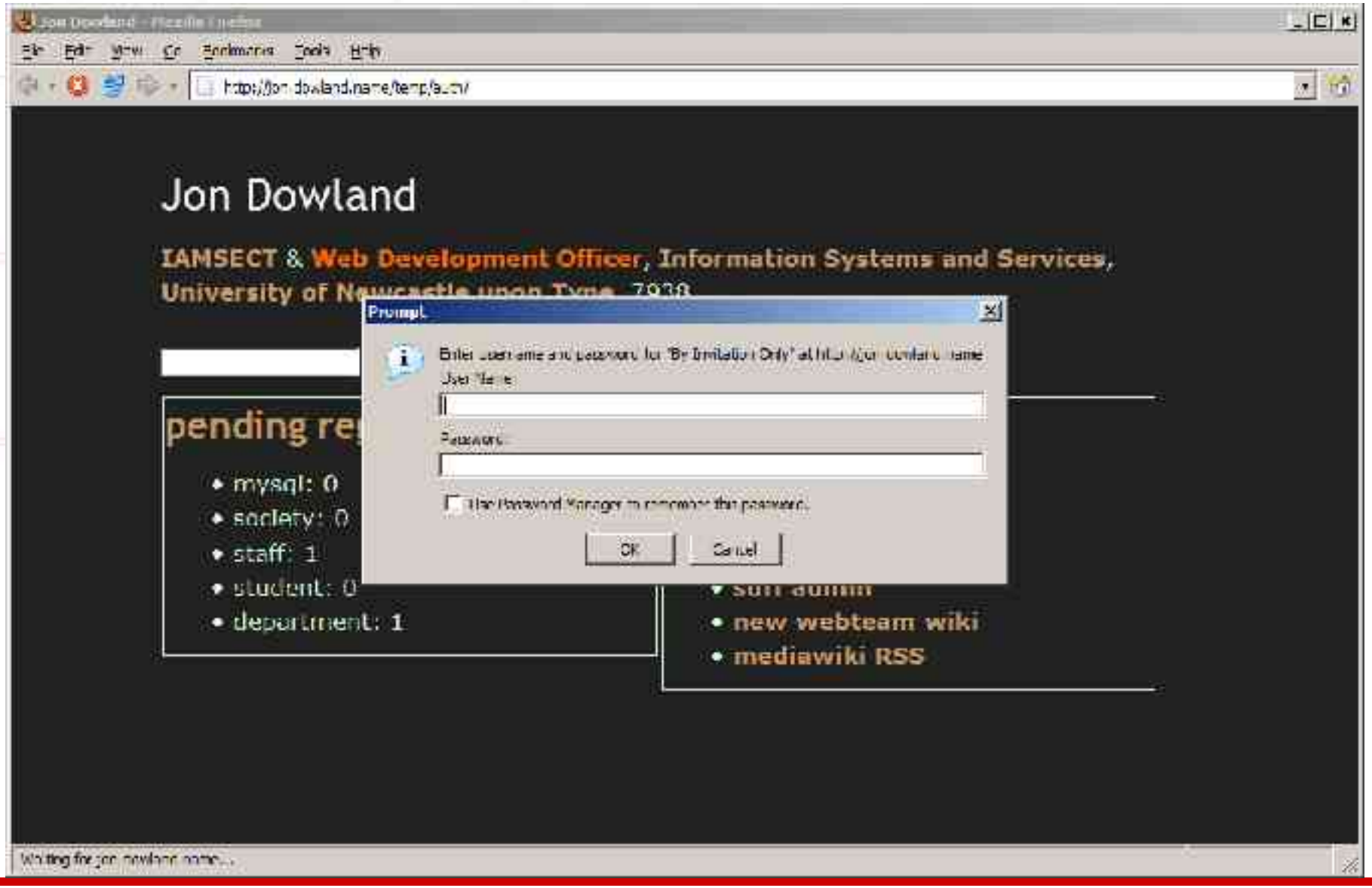
Single Sign-On solutions

- Pubcookie - http://www.pubcookie.org/
- Yale CAS - http://www.yale.edu/tp/auth/

Authentication/Authorisation

Existing approaches

HTTP Authentication (May 1996 or earlier)



```
>>>   GET /temp/auth/ HTTP/1.0

<<<   HTTP/1.1 401 Authorization Required
<<<   WWW-Authenticate: Basic realm="Invitation Only"
<<<   Content-Type: text/html
```

Browser prompts for username/password

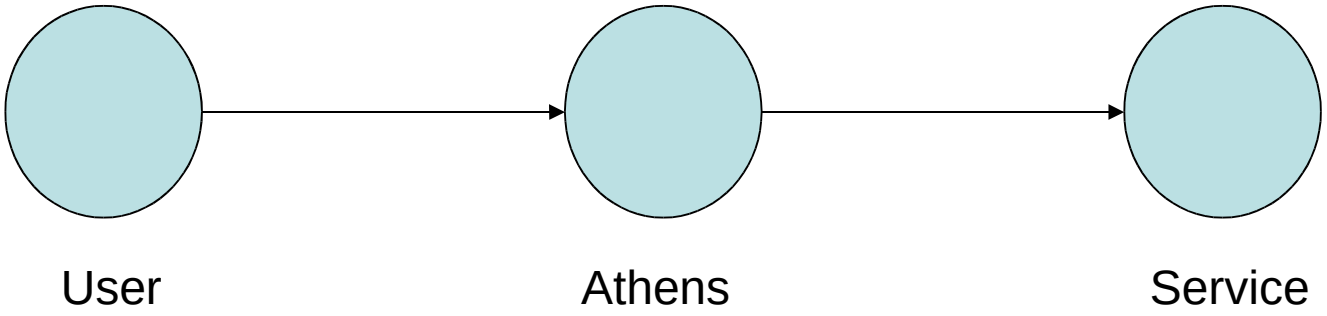
```
>>>   GET /temp/auth/ HTTP/1.0
>>>   Authorization: Basic xxxxxx

<<<   HTTP/1.1 200 OK
<<<   Content-Type: text/html
<<<
<<<   hello world
```

HTTP: Drawbacks

- Lack of ‘theme-able’ log-in
  - ‘help’
  - ‘mail me my password’
  - Etc.
- ‘Authorization:’ and authentication mixed-up
- Passwords sent in-the-clear
- No log-out mechanism

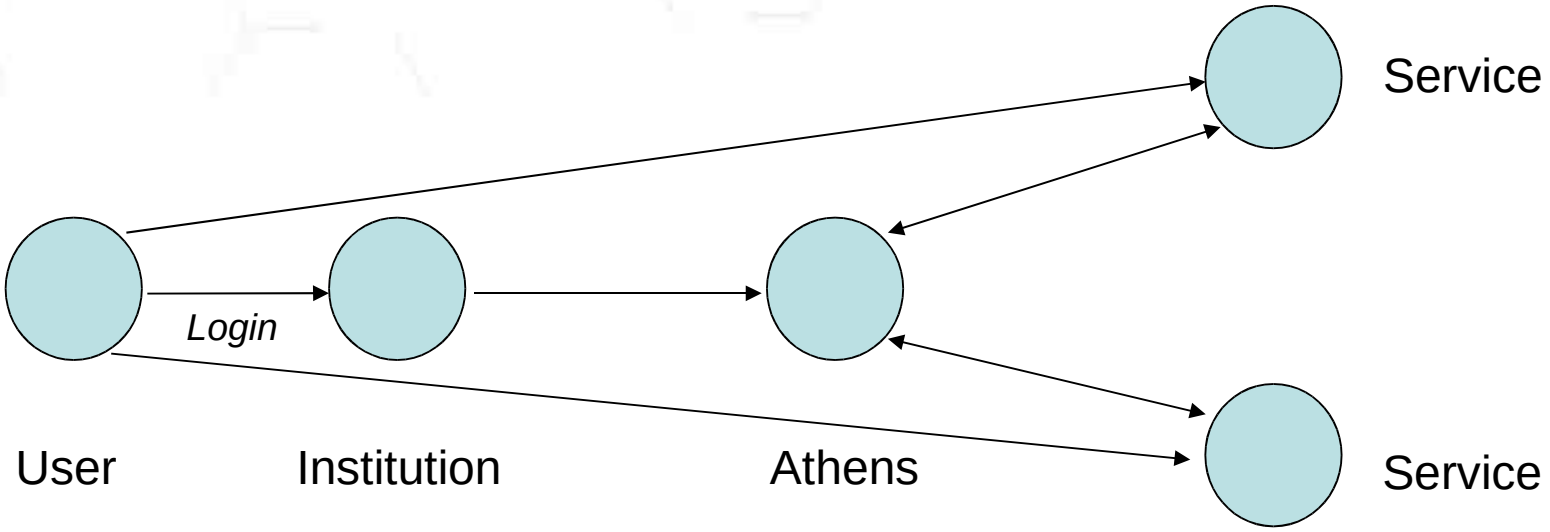
Athens (1996)

- Admired internationally, best of breed
- Single ID, multiple sign-on
- UK education and health
- Secure
- centralised



Athens D.A. (Oct 2002)

- Athens + SSO +
- devolved (locally managed) authentication



Athens services

ADITUS
AMADEUS
AMICO library
APU Library Proxy
Axiom
BANKSCOPE
BIDS CAB Abstracts
BIDS IBSS Service
BIDS Silver Platter INSPEC service
BIDS SilverPlatter PsycINFO Service
BLISS
BMJ Journals
BioMed Central
Blackwell-Synergy.com
British Standards Online
Business Ratio Reports
Butterworths Accountancy Direct
Butterworths All England Direct
Butterworths Banking Law Direct
Butterworths Businesscompliancedirect.co
Butterworths CaseSearch
Butterworths Civil Procedure Online
Butterworths Commercial Property Law
Butterworths Corporate Finance
Butterworths Corporate Law Direct
Butterworths Crime Online
Butterworths EBL Direct Essentials
Butterworths EBL Direct Premium
Butterworths EOR Direct
Butterworths EU Direct
Butterworths Employment Online
Butterworths Family and Child Direct
Butterworths Financial Regulations Servi
Butterworths Forms and Precedents Direct
Butterworths HSE Direct
Butterworths Halsbury's Laws of ...
Butterworths Human Rights Direct
Butterworths IRS Employment Review
Butterworths Immigration and Asylum Law
Butterworths Insolvency Law Direct
Butterworths Intellectual Property ...
Butterworths International Tax
Butterworths Law Direct
Butterworths Law Reports Direct
Butterworths Legal Updater
Butterworths Legislation Direct
Butterworths Licensing Direct
Butterworths Local Government Direct
Butterworths PI Online
Butterworths PensionsPro
Butterworths Property Tax Direct
Butterworths Scotland Direct
Butterworths Scots Law Direct
Butterworths Sergeant Sims Stamp Duty
Butterworths Stair Memorial
Butterworths Stone's Justices Manual
Butterworths Tax Direct
Butterworths Tax Planning Service
Butterworths Trusts and Estates Direct
Butterworths UK & International GAAPplus
Butterworths US Banking Editions Online
CHEST Associated Site Contacts
CHEST Further Education Site Contacts
CHEST Higher Education Site Contacts
CHEST Ireland Site Contacts
CSA Aqualine
CSA Artbibliographies Modern
CSA Internet Database Service
CSA Linguistics & Language Behaviour
CSA e-psyche
Cartalinx
Census Dissemination Unit
Census Geography Data Unit (UKBORDERS)
Census Interaction Data Service
Census Learning Resources
Census Microdata Unit at the CCSR
Census Registration Service
Chadwyck-Healey KnowEurope
Chadwyck-Healey KnowUK Database
Chadwyck-Healey LION for colleges
Chadwyck-Healey Literature Online
Chadwyck-Healey PCI Full Text Database
Childlink.co.uk
City University Virtual Library
Cochrane Library
Computer Abstracts
Creative Club
CrossFire Service (PLUSABGM)
CrossFire self-teach modules (MIMAS-XFT)
Dialog DataStar
Dialog Education@Site
Dialog@Site
EBSCOhost EJS
EBSCOhost databases
EDINA AGDEX
EDINA BIOSIS
EDINA BIOSIS Previews 1969 - 1984
EDINA CAB Abstracts
EDINA Compendex
EDINA Digimap
EDINA EconLit
EDINA INSPEC
EDINA Index to The Times, 1790 - 1980
EDINA MLA
EDINA PAIS
EDINA UPDATE
EEBO
EIU Citydata
EIU Countrydata
EIU Marketindicators & Forecasts
ESDS International
ESDU Data
ESRI NTF Converters
Education Image Gallery
Education Media OnLine
Education Media OnLine medical-restrict
Electronic Surgeons in Training Educatio
Emerald Fulltext
Emerald Management Reviews
Encyclopaedia Britannica
Engineering Village 2
Extenza e-Publishing Service
FAME
Gale Group InfoTrac
ISI JCR Science Edition
ISI JCR Social Sciences Edition
ISI Web of Knowledge
Idrisi
Ingenta Full Text Journals
Ingenta Select
Int. Civil Engineering Abstracts
Irish Reports and Digest
Isle of Man GIS data
JASPER
JUSTIS Celex and OJC
JUSTIS Daily Cases
JUSTIS ECJ Proceedings
JUSTIS Family Law
JUSTIS Hermes
JUSTIS Human Rights
JUSTIS Industrial Cases
JUSTIS Law Reports (eLR)
JUSTIS Law Reports Digest
JUSTIS Lloyd's Law Reports
JUSTIS Mental Health Law Reports
JUSTIS Official Journal C
JUSTIS Prison Law Reports
JUSTIS UK Statutes and SIs
JUSTIS Weekly Law
Jobs admin stuff
JustCite
Keynote
KumarandClark.com
LexisNexis
MD Consult
METAPRESS
MIMAS ISI BIOSIS Previews
MIMAS ISI Chemistry Server
MIMAS ISI Current Contents Connect
MIMAS ISI Derwent Innovations Index
MIMAS Infoterra
MIMAS Landmap
MIMAS Landmap Mediterranean
MIMAS LitLink
MIRA Virtual Automotive Info Centre
Martindale & Stockleys Drug Interactions
Mintel Reports
Mulberry
NeLH Evidence-Based on Call
NeLH Journal of Medical Screening
NetLibrary
NewsBank InfoWeb
OCLC FirstSearch Service
OSIRIS
Ovid Online
Oxford English Dictionary Online
Oxford Reference Online
Papyrus software for DOS
Papyrus software for the Mac
Parlianet
Perfect Analysis
Primal Pictures Basic Anatomy (NHS)
Primal Pictures anatomy.tv
ProQuest
ProQuest Reference Asia
RCS Affiliates Area
RCS Discussion Fora
RCS Library Electronic Journals
RCS Members Area
RefWorks
Reuters Business Insight Unlimited
SCOTBIS: Members Area
SCRAN Web Site
ScienceDirect
Sentient DISCOVER
SilverPlatter Arc2
Snapshots International: Market Research
Statistical Accounts of Scotland
SwetsWise
Synsoft HYDRA and HYDRA ONLINE
TRILT
Taylor and Francis eBook Subscriptions
Technical Indexes Info4Education
Technical Indexes Info4HealthEstates
The Academic Library
The Times Law Reports
UK JSTOR Mirror Service
WILSONWEB
Westlaw UK
Wiley InterScience
WriteNote
XpertHR
ZETOC - BL Electronic Table of Contents
eSTEP administrators resource
images.MD
xreferplus

Shortcomings

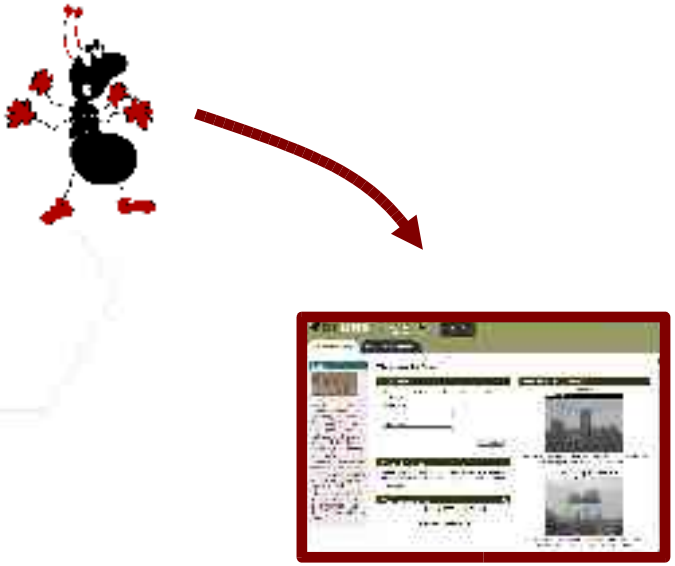
Shortcomings

- Usage statistics
- Bureaucracy and ad-hoc groups (VRGs)
- Fine-grained access control
- Privacy and anonymity
- Reluctant international services

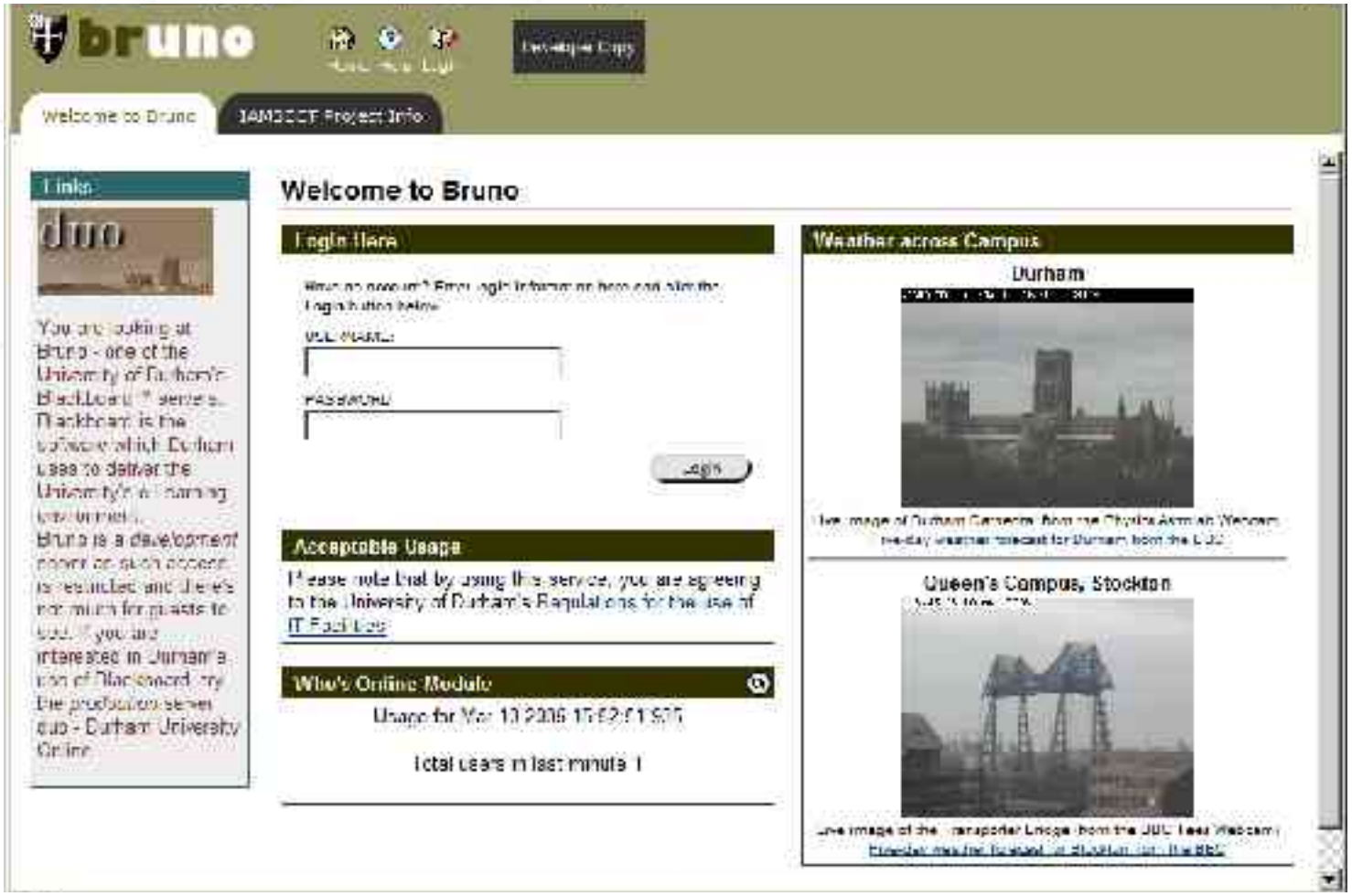
Shibboleth is…

detailed demo

User attempts to access service



http://bruno.dur.ac.uk/



Interlude: where are they from?

- Autodiscovery (e.g. by host)

- Manual

Interlude: where are they from?

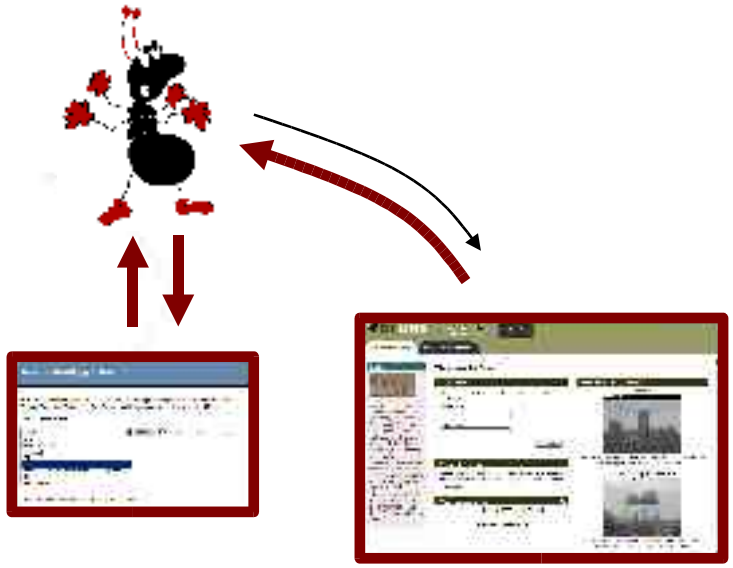
- Autodiscovery (e.g. by host)

  Unreliable
  we're trying to *simplify* the service provider

- Manual

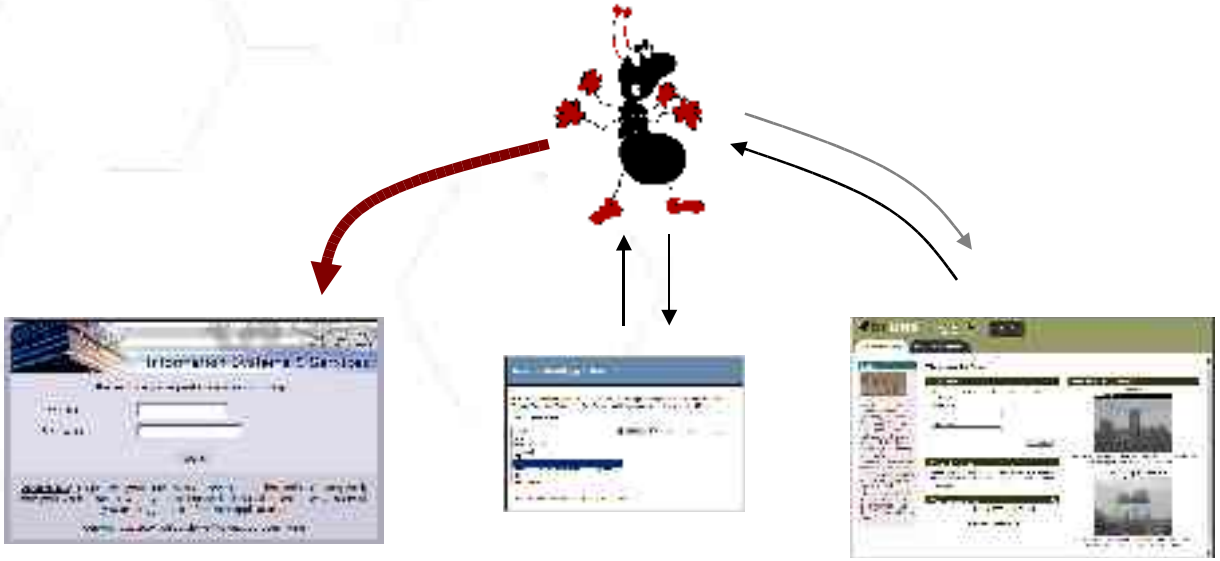
  Simple
  User burden

User redirected to “WAYF”



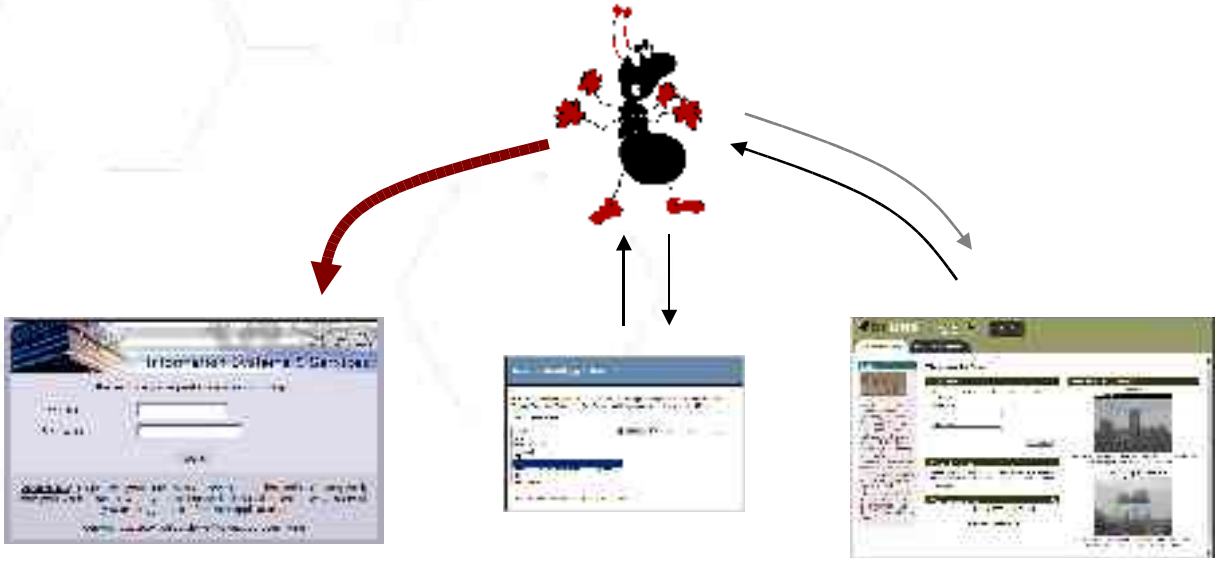
https://wayf.sdss.ac.uk/shibboleth-wayf/...

User directed to “home”

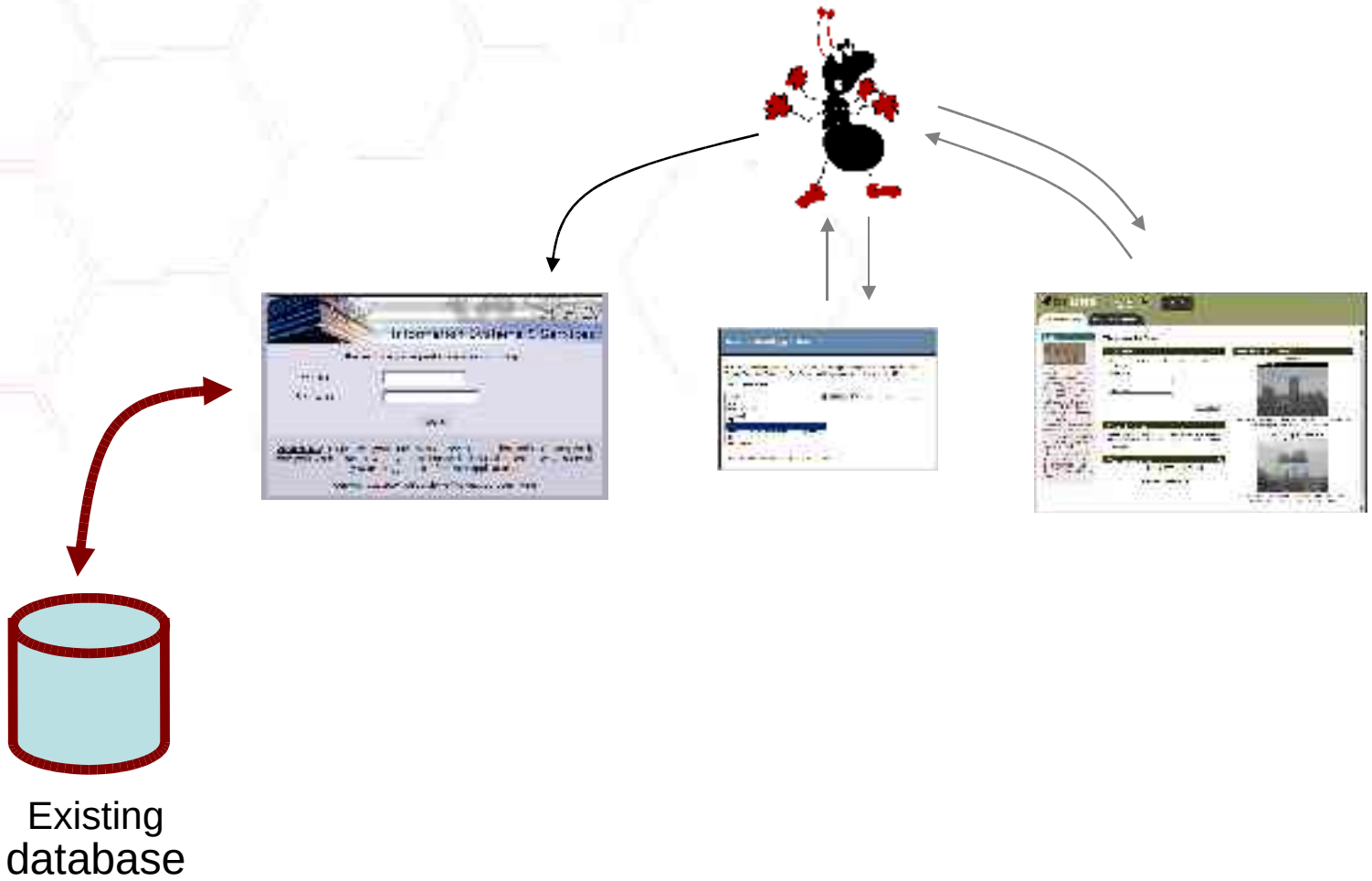


https://weblogin.ncl.ac.uk/cgi-bin/index.cgi

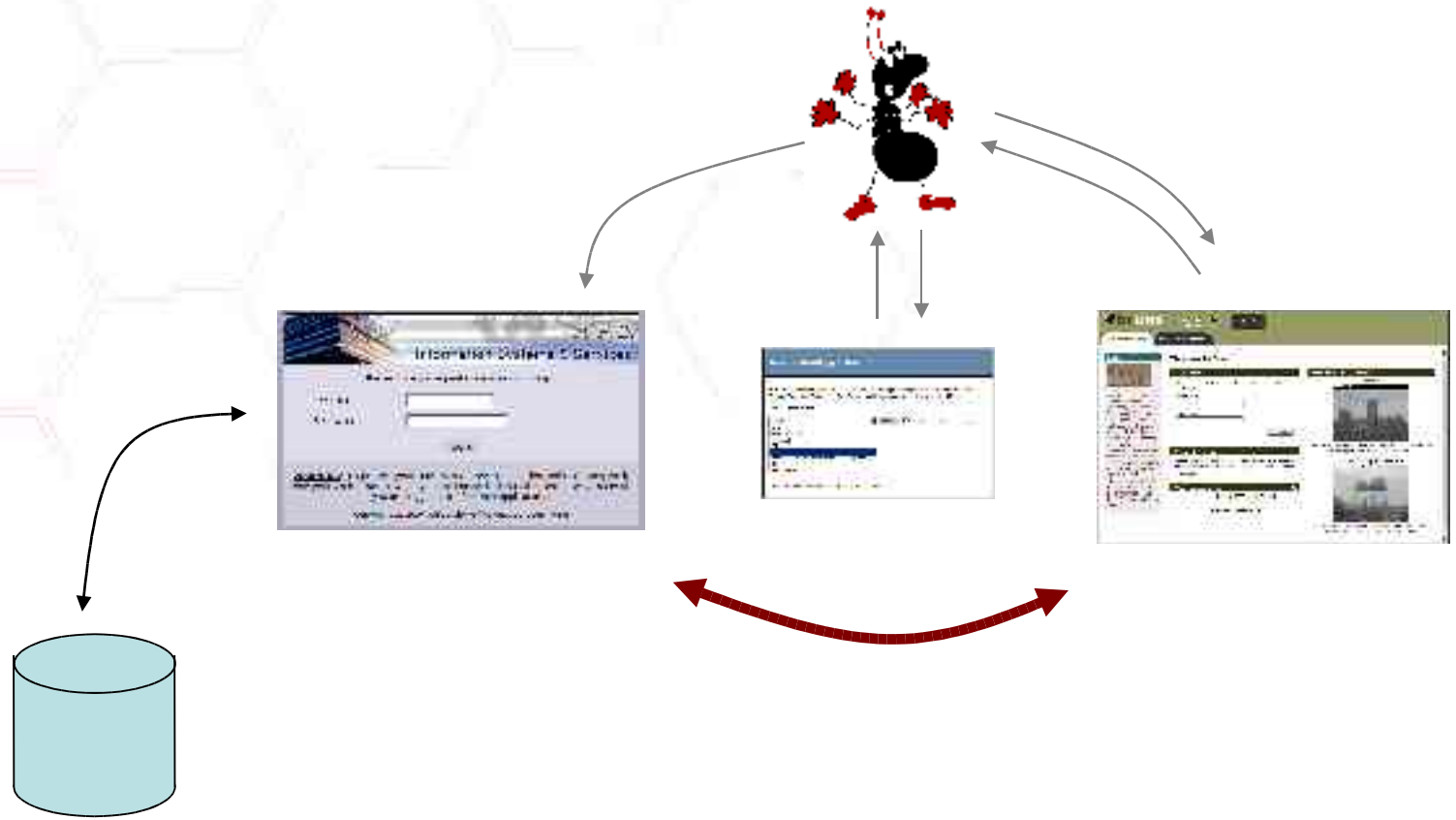
User provides credentials



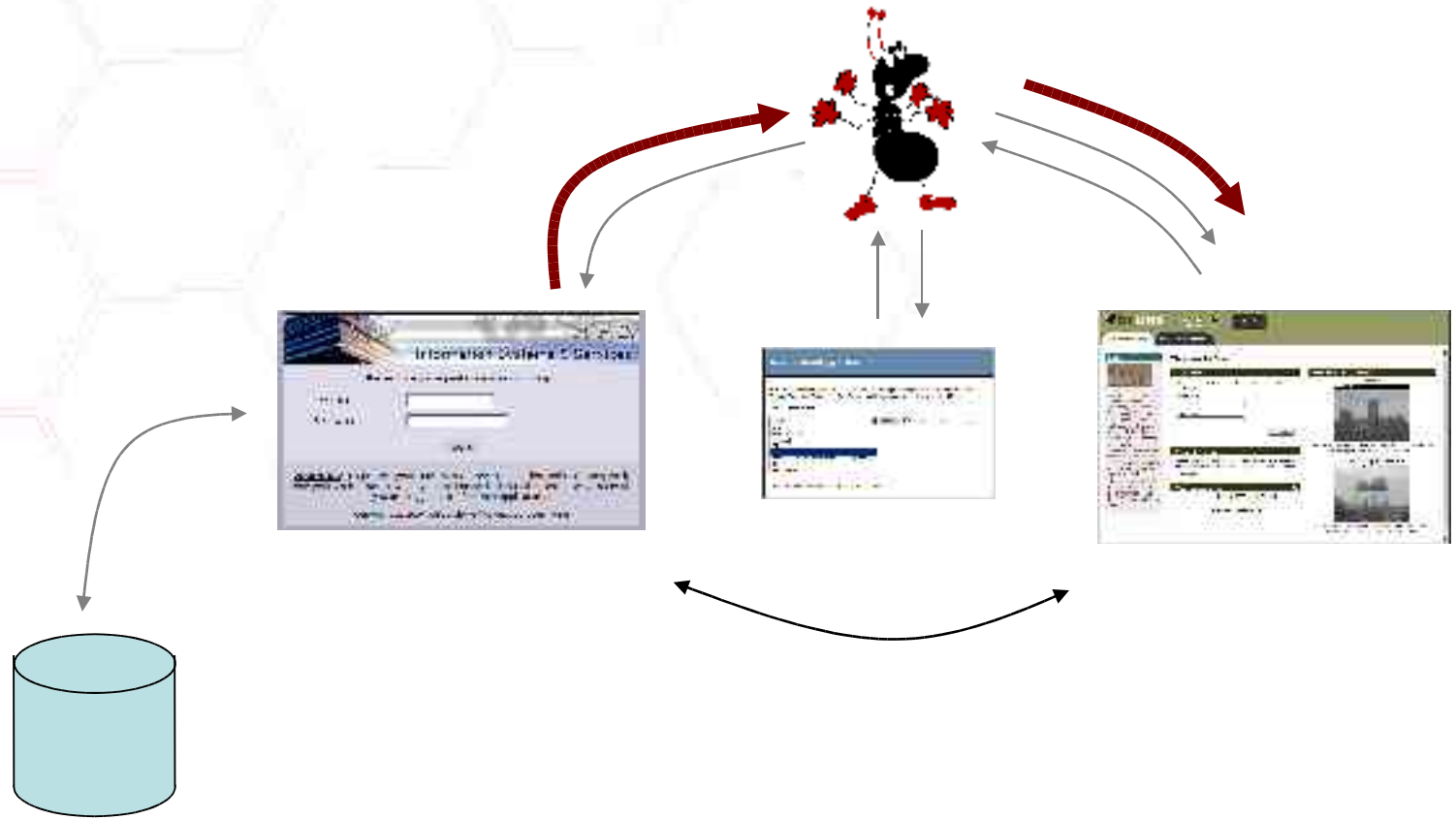
“home” authenticates user



Attributes are exchanged



User directed to service



From the flyer

*"Shibboleth is a **fine-grained** authorization framework which separates responsibility for **authenticating** a user from the responsibility of **authorizing** their access to a resource."*

Who someone is

Authentication ≠ Authorisation

What someone can do

Authentication

Identity Provider

Authentication

Identity Provider

- home institution
- trusted

Identity Provider

- home institution
- trusted

Attribute Exchange

Case studies

Case Study	Attribute
• Course specific sensitive material	• Enrolled courses!

Case studies

Case Study	Attribute
• Fully-private, anonymous access	• Nothing!

Identity Provider

- home institution
- trusted

- Secure
- Pre-agreed information

Attribute Exchange

Identity Provider

- home institution
- trusted

Service Provider

- Secure
- Pre-agreed information

Attribute Exchange

Identity Provider

- home institution
- trusted

Service Provider

- No user database
- No synchronization issues

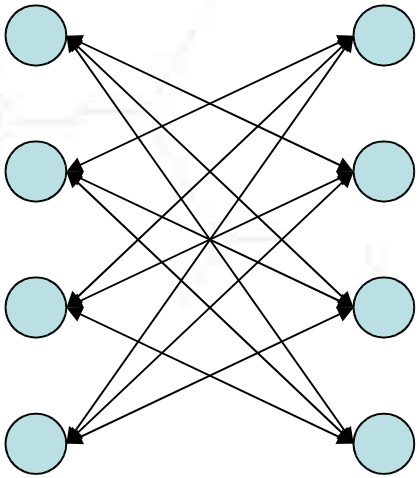
- Secure
- Pre-agreed information

Attribute Exchange

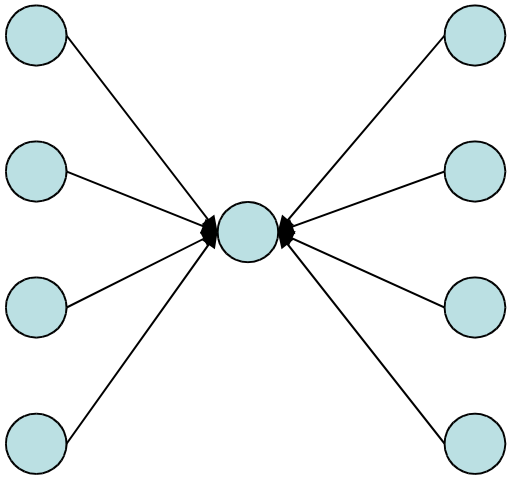
Terminology: Federations

?

Simplified relationships



24 relationships



8 relationships

Example Federations

- InQueue
- InCommon
- Athens
- SDSS

Who’s doing what

U.S.

- Internet2 consortium
- Incommon federation
  - 16 universities
  - 4 others

Around the world

- Switzerland – SWITCH
- Finland – HAKA

- Australia, Hungary, Croatia deploying

- Rest of Europe: contemplating

U.K.

- BECTA – ICT/schools
  - Shibboleth pilot
- JISC
  - Core middleware
  - Distributed e-learning
  - Early adopters
  - …

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

- JISC Core Middleware

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

Inter-institutional

- Collaboration
  - Durham
  - Newcastle
    - Web team
    - Faculty of Medical Sciences
  - Northumbria

Authorisation, Clinical Teaching

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

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

- Shared students

Medicine and Surgery

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 in the Fact File when completing your UCAS form.)

Course content: The course is split into two Phases. Phase 1, 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 1 pathways share common outcomes, with the quality of teaching being excellent at both institutions. Following completion of Phase 1, 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

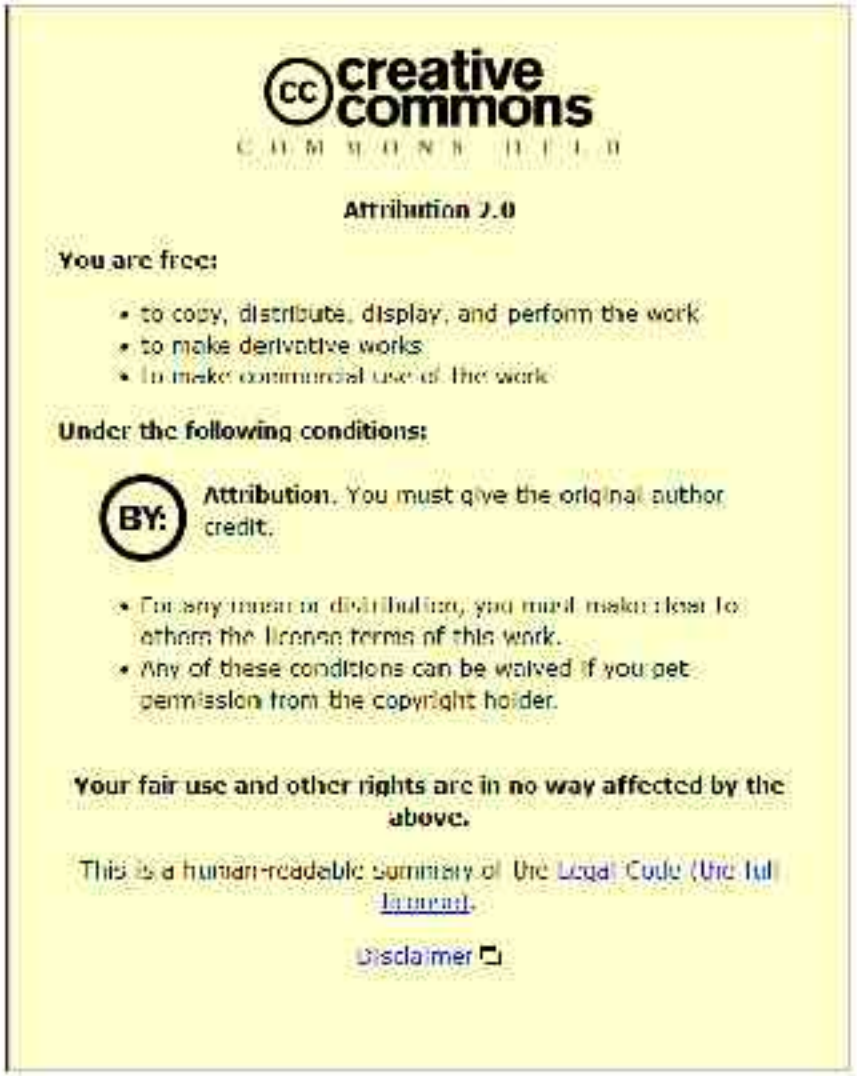
Authorisation, Clinical Teaching

- In-house medical-oriented virtual learning environment (VLE)

What we've done (1)

- Technical-oriented guides
  - Local SSO (pubcookie)
  - Shibboleth Identity Provider
- Creative Commons

Creative Commons



What we've done (2)

Techie

- Shibboleth origin installation
- Shibboleth target installation
- target/zope integration
- federation testing

What we've done (3)

Non-techie

- Glossary
- Questionnaire
- Dissemination

What we're doing

- Further Zope-based VLE work
- Blackboard VLE
- Managerial documentation
- Further events

Future guides (1)

How to identify attributes, attribute stores

- Which attributes are useful
- Identifying stores
- Pros and con of store types

Future guides (2)

A managerial guide to getting shib

- what skill set you need in your team
- Privacy & data protection issues
- Certificate provider issues
- Negotiating in a federation

What *other* people are doing

- SDSS – development federation
- AMIE – distributed attribute management
- PERSEUS – Shibboleth and portals
- GUANXI – Bodington VLE

- **http://www.jisc.ac.uk/index.cfm?name=programme_middleware**

Summary

- State of the art has drawbacks
- Shibboleth might address them
- Lots of work taking place

Questions