



# 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



Shibboleth is a Single Sign-On (SSO)  
solution

# Statement



Shibboleth is a Single Sign-On (SSO)  
solution

**Myth**

# Single Sign-On solutions

---

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

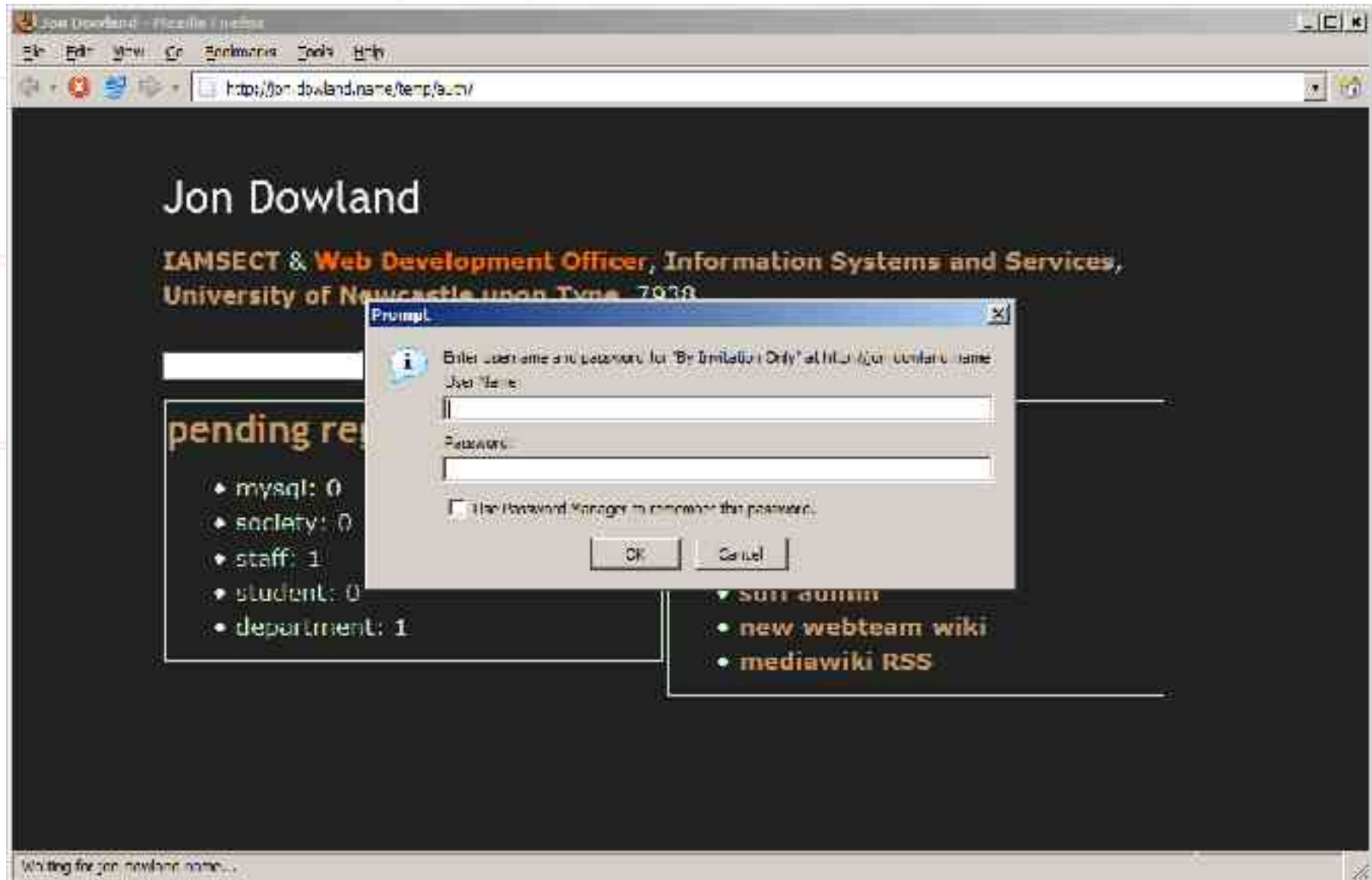




# Authentication/Authorisation

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 xxxxxxx
```

```
<<< HTTP/1.1 200 OK
```

```
<<< Content-Type: text/html
```

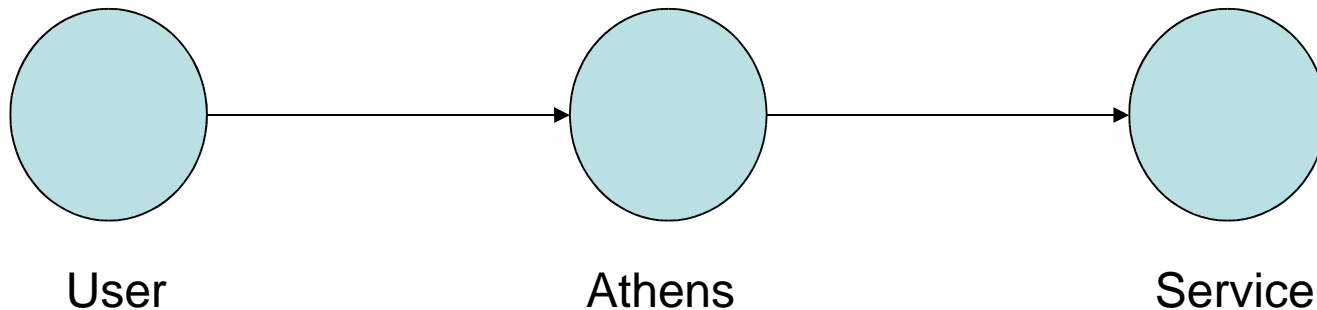
```
<<<
```

```
<<< hello world
```

- 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

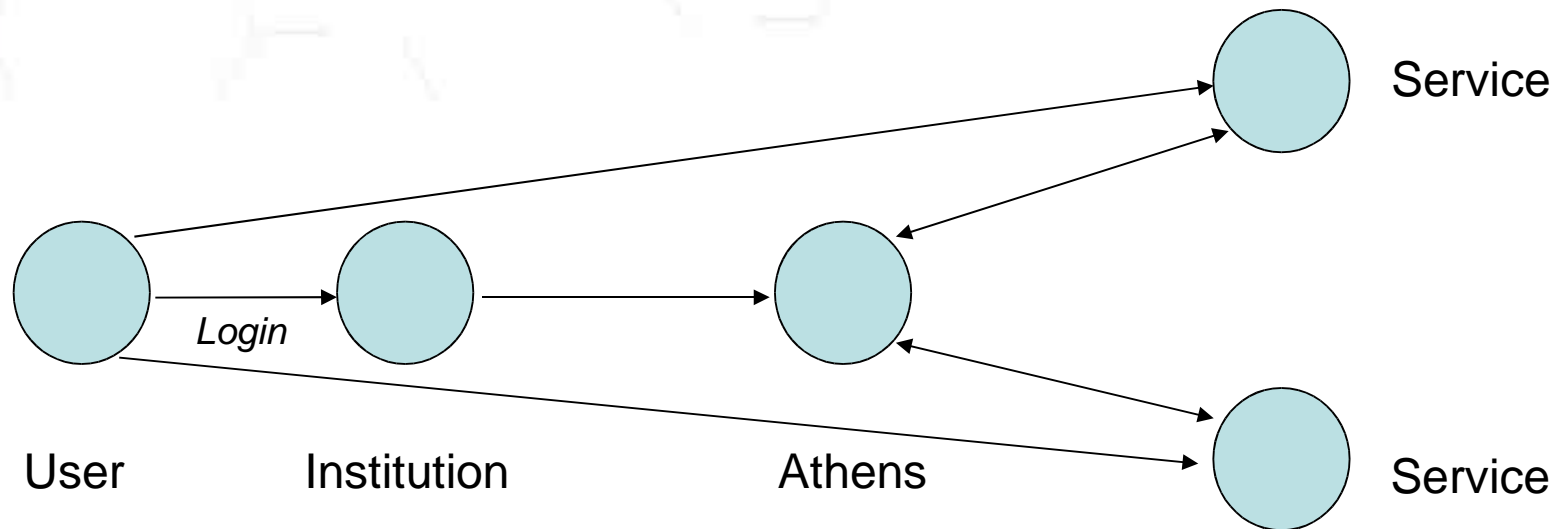
# Athens (1996)

- 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 Businesscomplianceirect.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-psych  
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  
Ildrisi  
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 staff  
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  
Parliant  
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



The screenshot shows the Bruno website interface. At the top, there is a header with the Bruno logo, navigation icons, and a 'Language Copy' button. Below the header, there are two tabs: 'Welcome to Bruno' and 'IAMSECT Project Info'. The main content area is divided into several sections:

- Links:** A section with a 'duo' image and a paragraph of text: "You are looking at Bruno - one of the University of Durham's Blackboard™ series... Blackboard is the software which Durham uses to deliver the University's e-learning content... Bruno is a development point on such access is restricted and there's not much for guests to see... If you are interested in Durham's use of Blackboard, try the production server duo - Durham University Online."
- Welcome to Bruno:** A section with a 'Login Here' header. It contains a login form with fields for 'FULL NAME:' and 'PASSWORD:', and a 'Login' button. Below the form, there is a paragraph: "When an account's first login information has been set, the Login button below..."
- Acceptable Usage:** A section with a header and a paragraph: "Please note that by using this service, you are agreeing to the University of Durham's Regulations for the use of IT Facilities."
- Who's Online Module:** A section with a header and a paragraph: "Usage for Mon 13 2006 17:52:51 GMT". Below this, there is a counter: "Total users in last minute: 1".
- Weather across Campus:** A section with two sub-sections: "Durham" and "Queen's Campus, Stockton". Each sub-section has a live image and a caption: "Live image of Durham Campus from the Physics Arm in Western" and "Live image of the Transponder Bridge from the JCU Teak Webcam".

# Interlude: where are they from?

---

- Autodiscovery (e.g. by host)
- Manual

# Interlude: where are they from?

---

- Autodiscovery (e.g. by host)

Unreliable

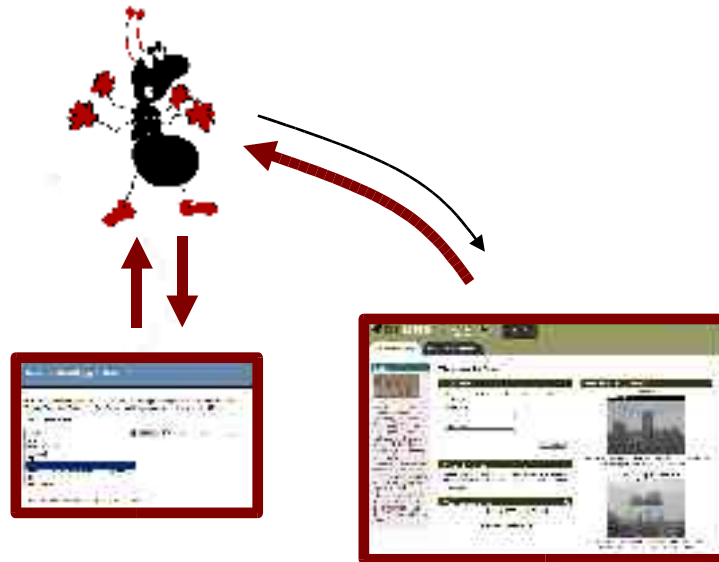
we're trying to *simplify* the service provider

- Manual

Simple

User burden

# User redirected to "WAYF"





**Select an identity provider**

In order to fulfil the request for a web resource you have just attempted to access, information must be obtained from your identity provider. Please select the provider with which you are affiliated.

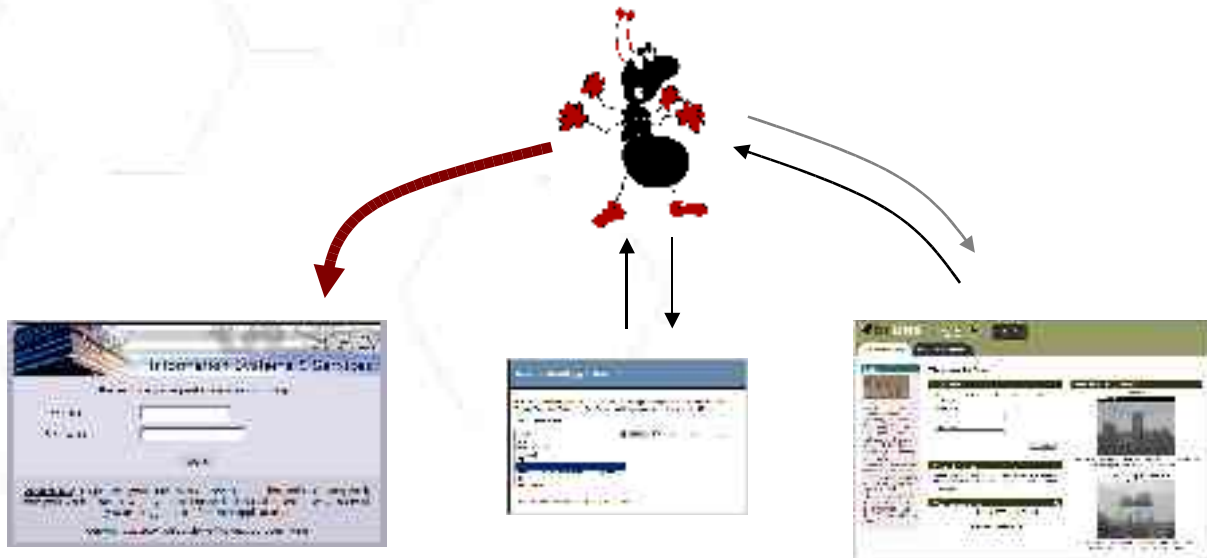
**Choose from a list:**

AMIE   Remember my selection on this computer.

- AME
- AME\_AUTHZ
- icy.org.uk
- LSE
- Newcastle**
- Oxford University Computing Services (Test)
- SDSS
- SDSS Nevis

Need assistance? Visit the [SDSS Federation web site](#)

# User directed to "home"





Home Contact Search

## Information Systems & Services

The resource you requested requires you to login.

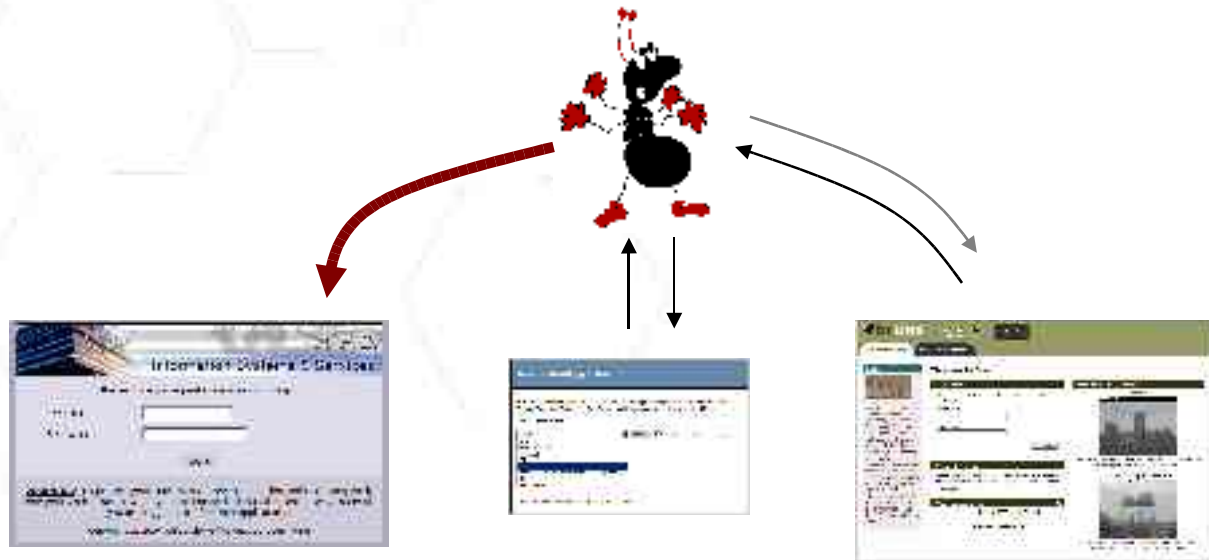
User ID

Password

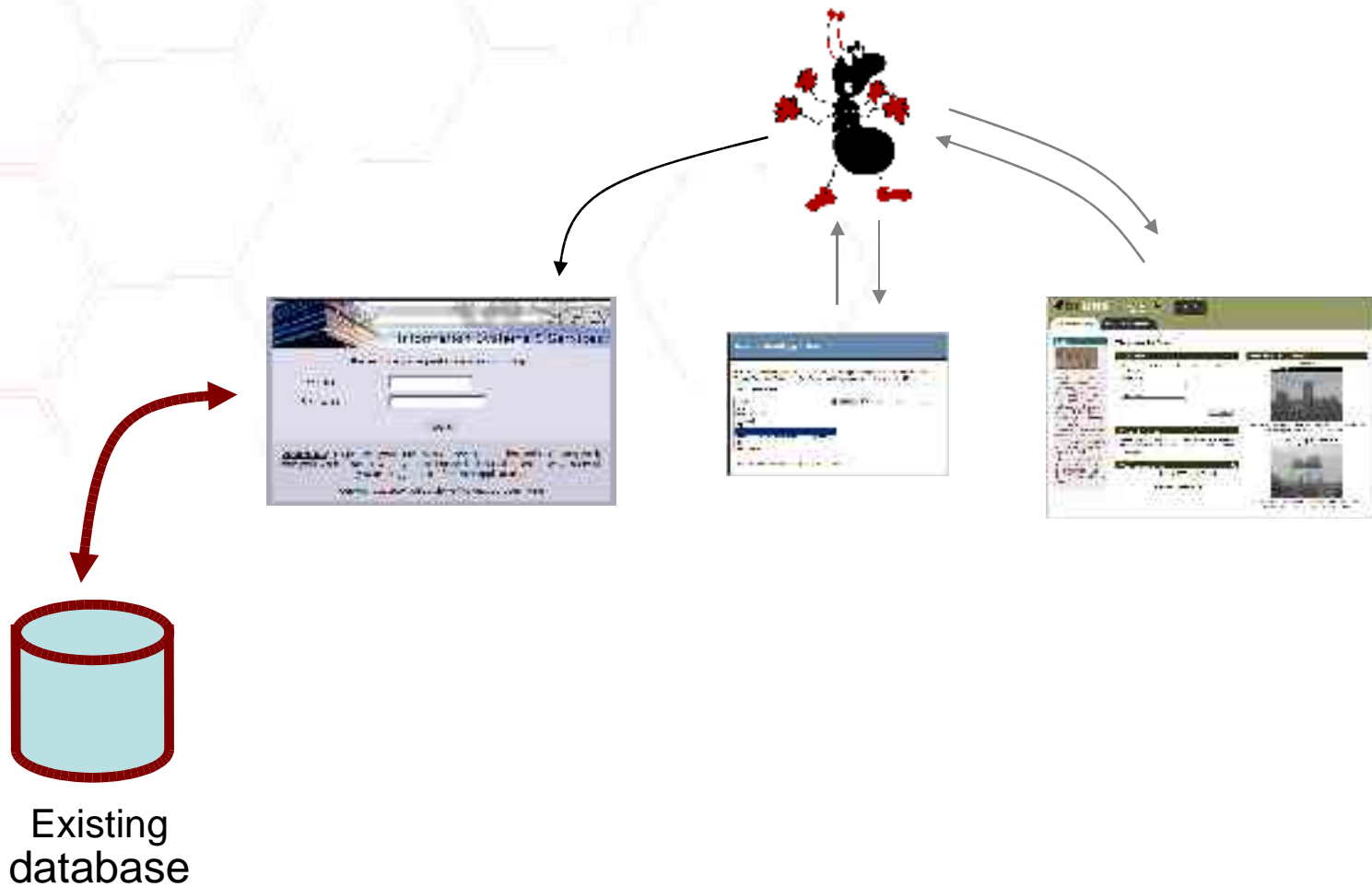
**WARNING:** To protect your privacy and prevent unauthorized use, completely close your Web browser when you are finished. This is the easiest way to ensure you are logged out of all web applications.

Copyright © 2004 University of Newcastle upon Tyne

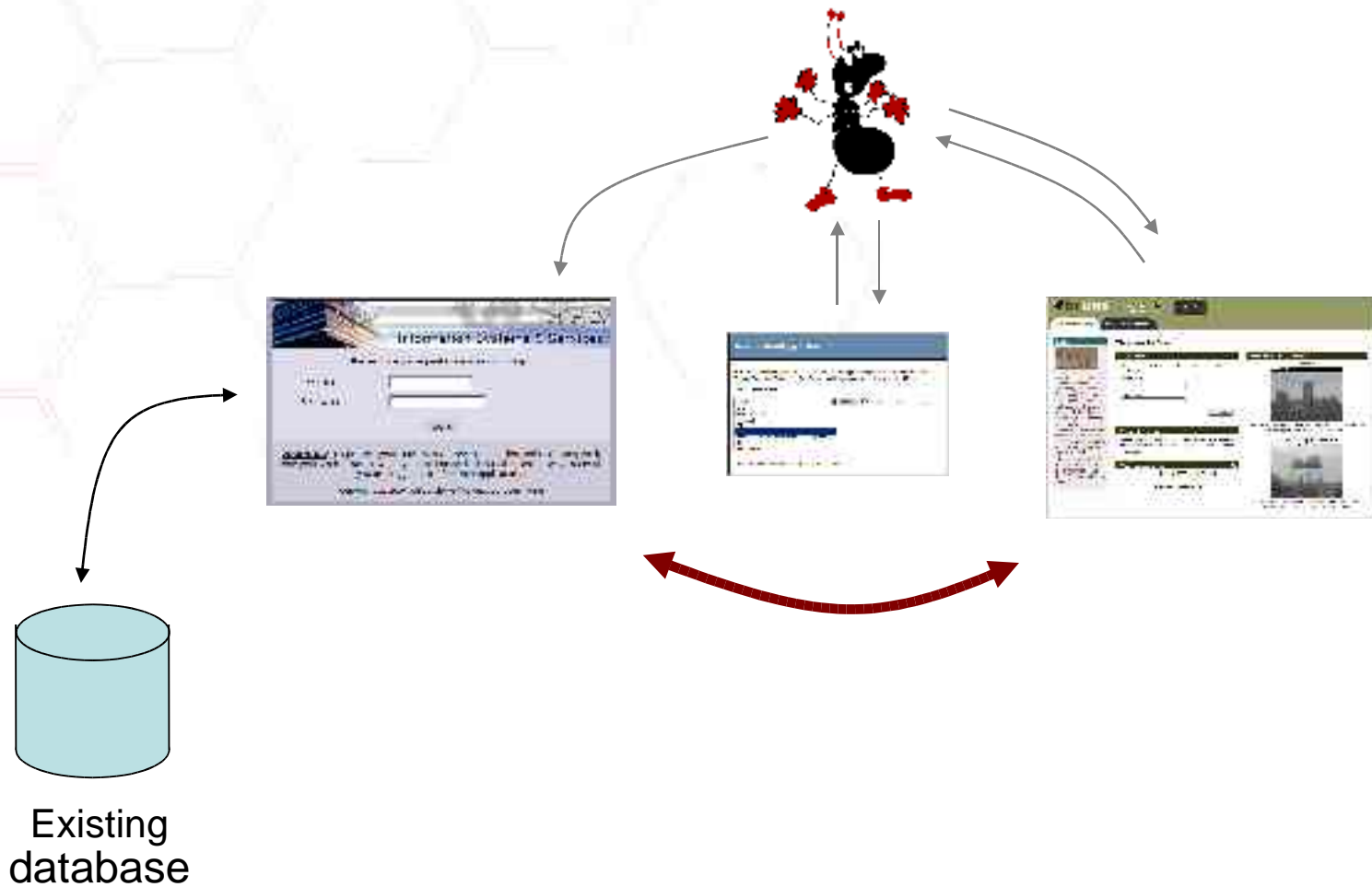
# User provides credentials



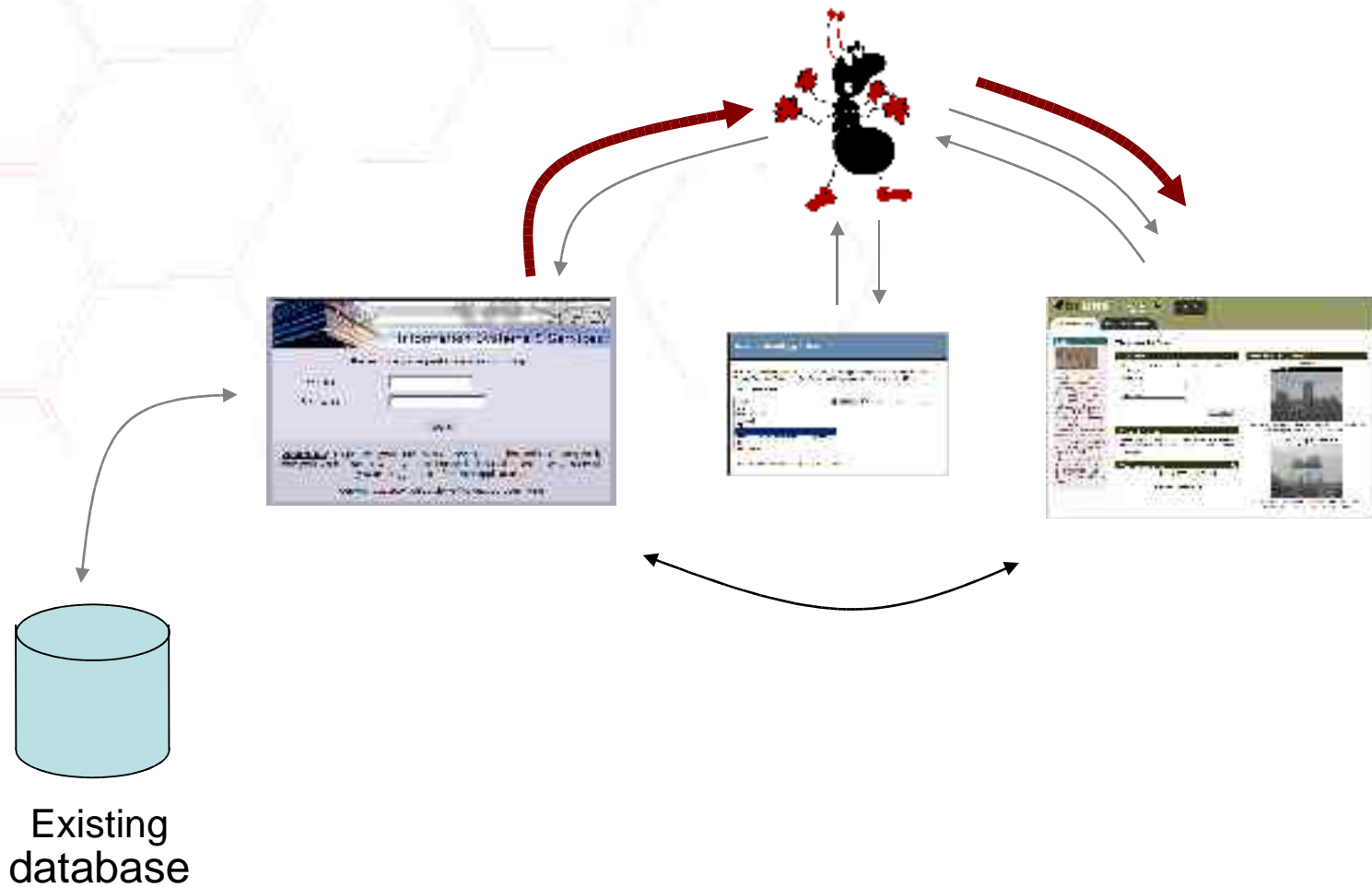
# “home” authenticates user



# Attributes are exchanged



# User directed to service



*“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  $\neq$  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

- Course specific sensitive material

## Attribute

- Enrolled courses!

# Case studies

---

## Case Study

- Fully-private, anonymous access

## Attribute

- 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

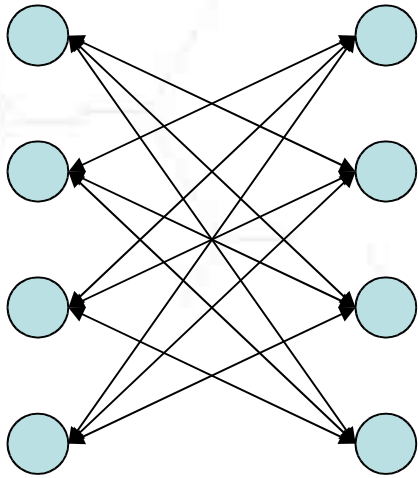


# Terminology: Federations

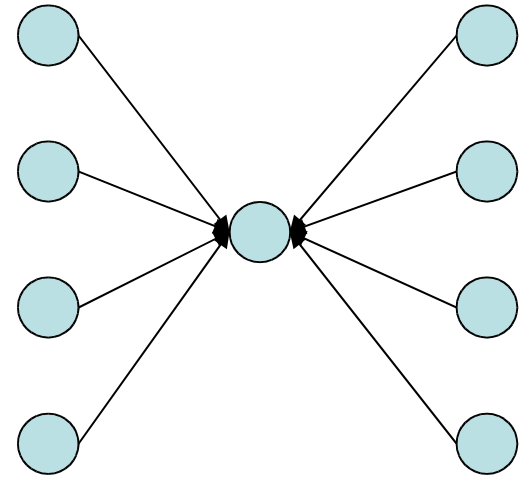
?

# Federations

## Simplified relationships



24 relationships



8 relationships

# Example Federations

---

- InQueue
- InCommon
- Athens
- SDSS



Who's doing what

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

# Around the world

---

- Switzerland – SWITCH
- Finland – HAKA
- Australia, Hungary, Croatia deploying
- Rest of Europe: contemplating

- 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/>

- 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

- Shared students

Medicine and Surgery MBBS (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 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 pathway for the three years of Phase 2, which

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 courses are there?

- 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



## Attribution 2.0

### You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

### Under the following conditions:



**Attribution.** You must give the original author credit.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

**Your fair use and other rights are in no way affected by the above.**

This is a human-readable summary of the [Legal Code \(the full legal text\)](#).

[Disclaimer](#) 

# 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](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