

Shibboleth and the **iamsect** Project

Introduction



Overview

Morning session:

History of access control

Current solutions

Problems with current solutions:

- For users
- For administrators

The solution: Shibboleth

Where the IAMSECT project fits

How to prepare for shibboleth

Afternoon session: Guest speakers



History

Access control to library resources

The pros and cons of each era

- The paper era
- The rise of electronic media
- The rise on online systems

Focus on access control, user experience and administrator experience.



Early days of journal provision

The era of Paper on shelves

No real access control

Librarian and user face to face

Sensitive material behind the desk

e.g. Derbyshire put “The Sun” behind the desk, videos in the Walton library

Logistical Problems:

- Need physical copy, generally shared
- User need to journey to library to get access
- Library has to maintain journals
- No real usage stats



The start of electronic journals

Journals kept as locally held databases or cd-roms
No real access control

Again logically difficult

- Need physical copy or dedicated machine
- User need to journey to library to get access
- Library has to maintain cd roms and database
- No real usage stats



Online journals

Available since 1996

Mainly lists of article titles and abstracts
some full text

Lessens need for inventory

Largely reliant on service providers for stats

User does not need to be present, may need
to be on campus



Early online access control

IP address checking

Useful, easy to do, but crude

Authenticates machines not people

Unhelpful when the users population is
mobile (EZproxy can help...a bit)

Discipline of abuse can damage innocents



electronic access control

Individual usernames and passwords
.htaccess, individual databases

Good fine grained control

- each user has own username and password.

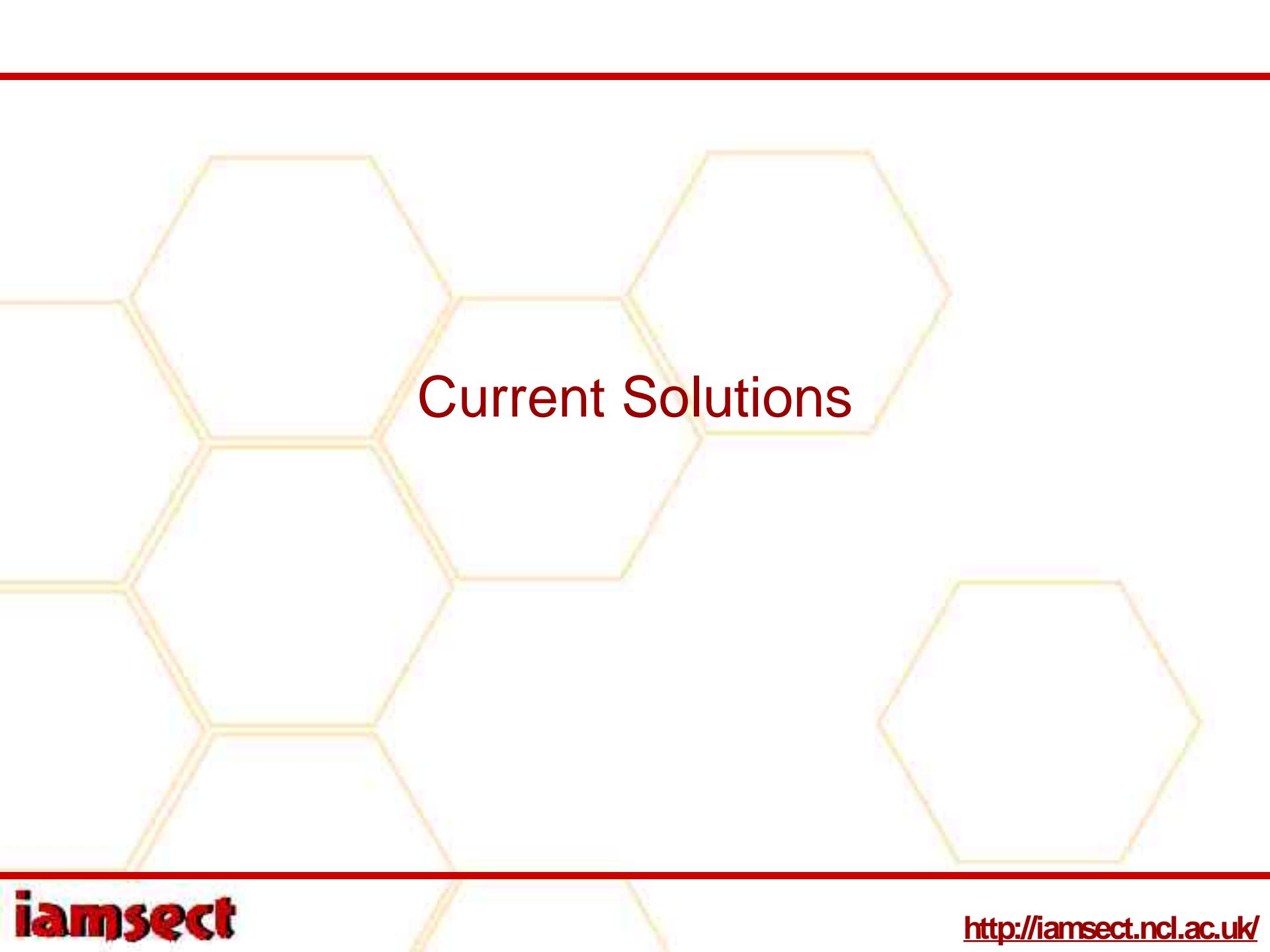
Burden on the user is high

Burden on administrators is high

Doesn't scale well:

- easy for 20 users
- nightmare for 1000

Insecure

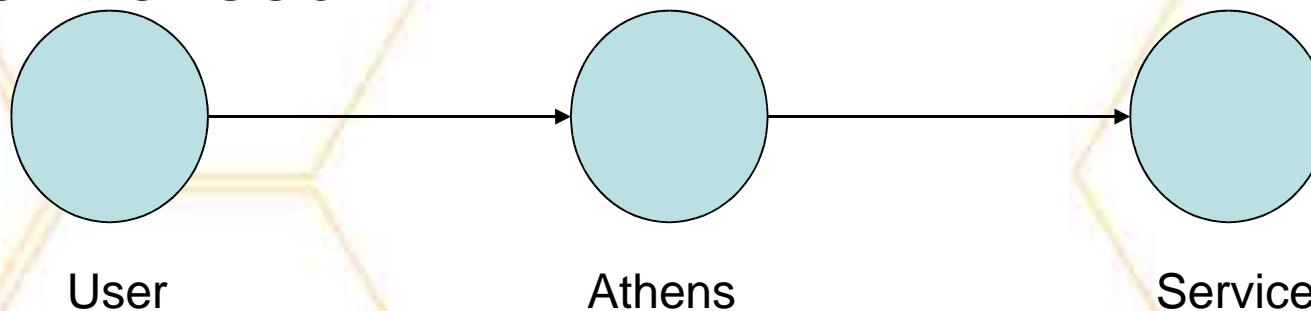


Current Solutions



Athens (1996)

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





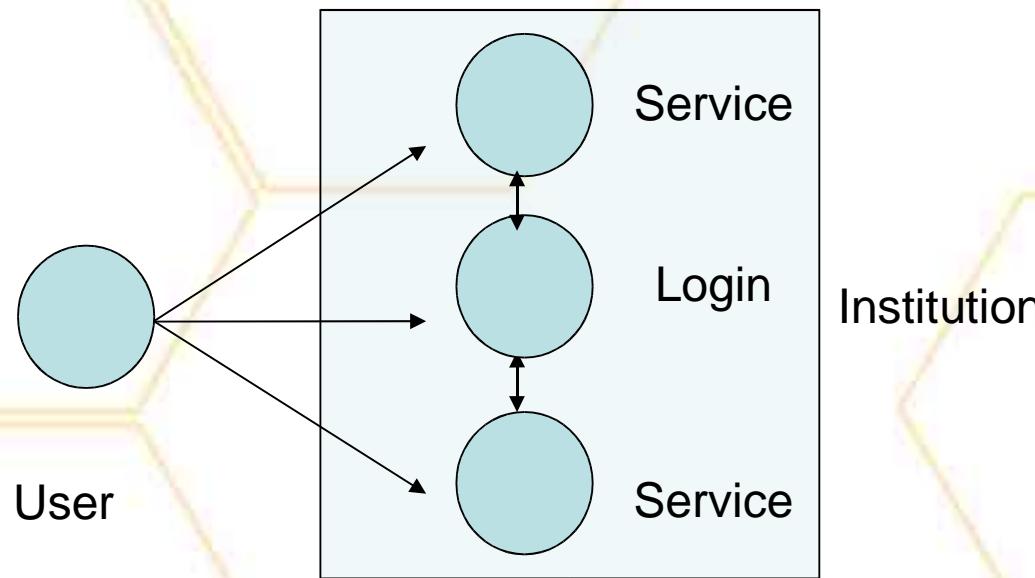
Single Sign-On

- User convenience: login once per session
- Authentication managed behind the scenes



Single Sign-On

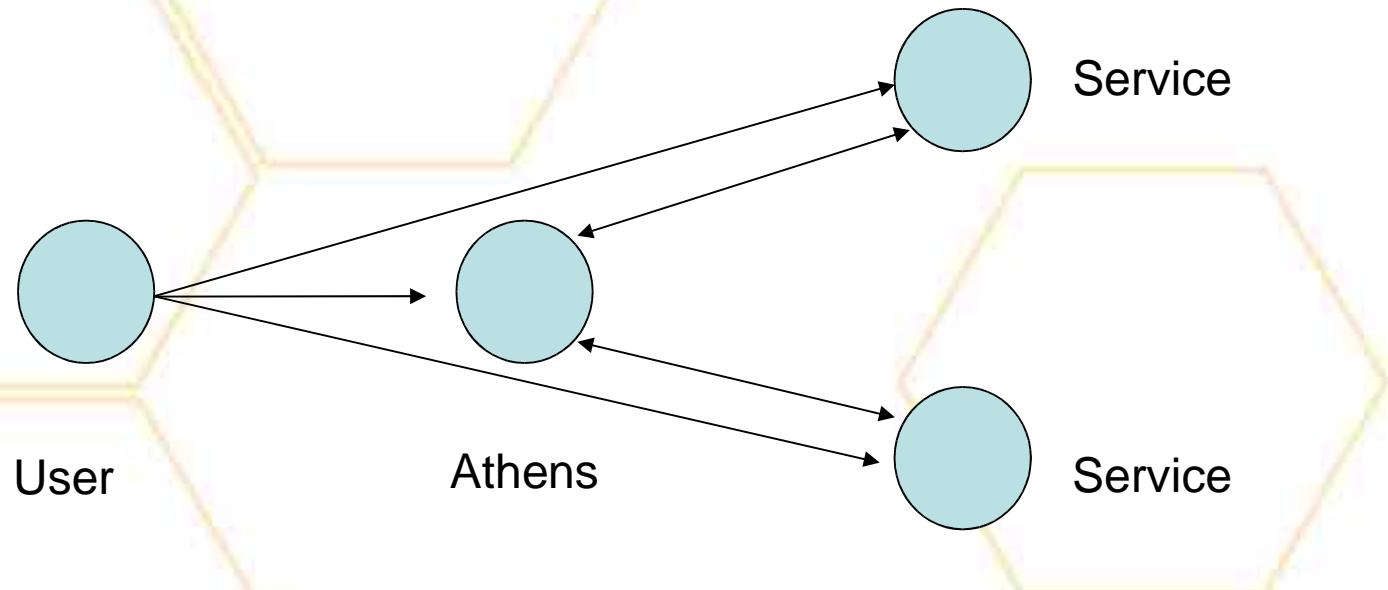
- E.g.
 - Pubcookie
 - Yale central authentication service
- (Shibboleth builds on these)





AthensSSO (Feb 2002)

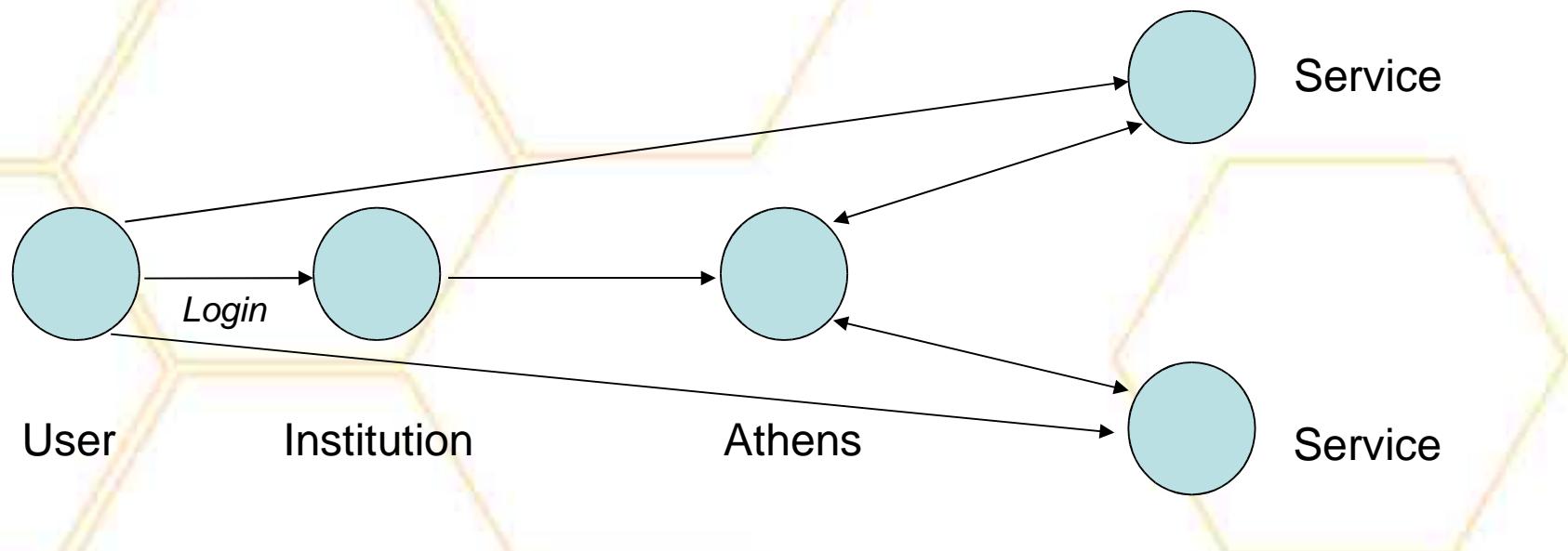
- Athens, +
- Single sign-on

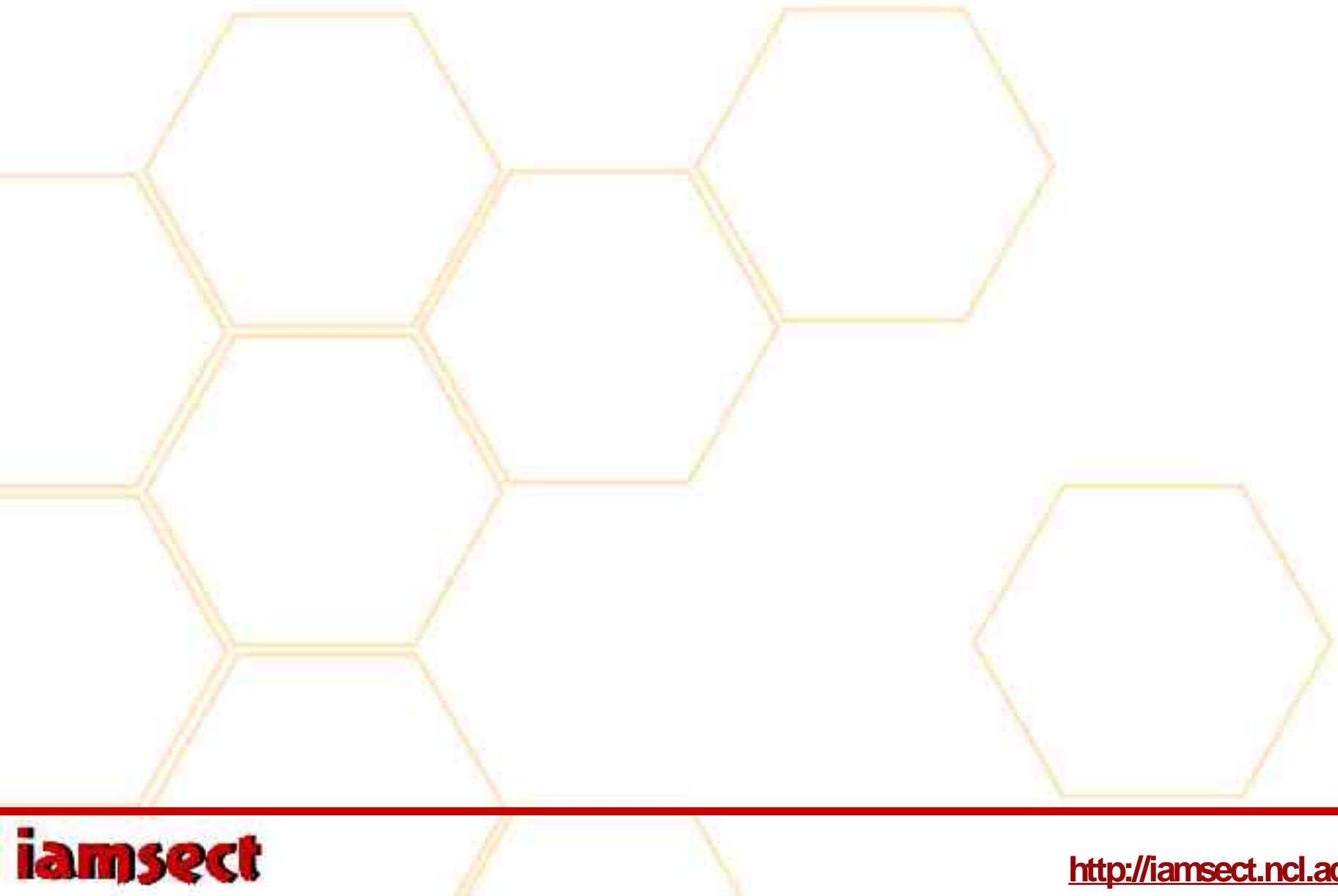


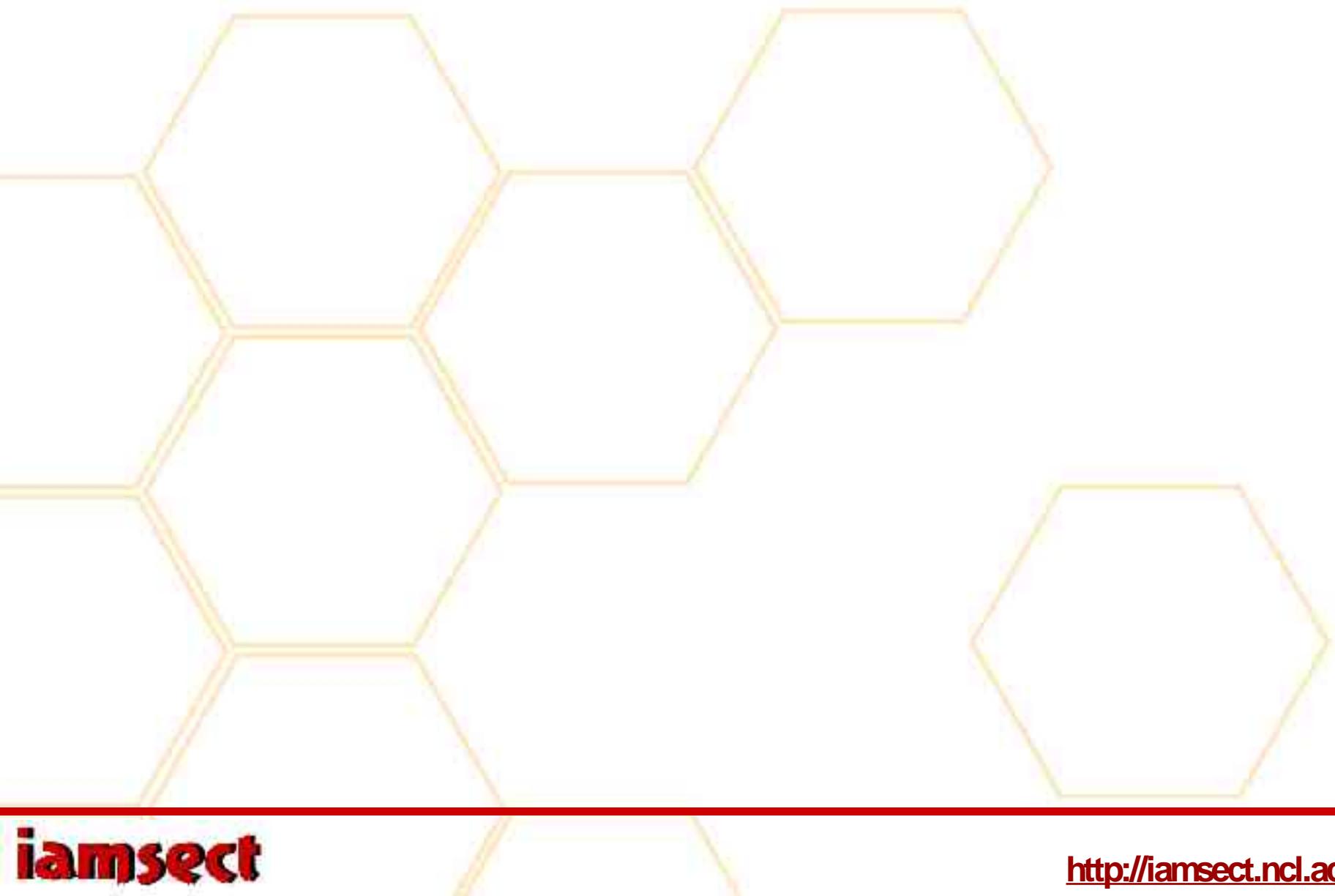


Athens D.A. (Oct 2002)

- AthensSSO, +
- devolved (locally managed) authentication









The concepts of access control

The difference between authentication and authorisation

Physical access control

Virtual access control

User experience

Administrator experience



Authentication and Authorisation

Authentication

Identifies who you are

Authorisation

Once who you are is known, identifies what you are allowed to do.

Historically have been treated as the same the thing



Authentication/Authorisation Examples

Keys identify you and authorise you at the same time.....tied to the bearer

Passport identifies you, passport control authorises you.

Computer login identifies you, permissions in system authorise you



Different authentication methods

Physical tokens:

- Keys
- Cards (swipe, chip 'n' pin, etc.)

Virtual tokens

- Pin numbers
- Username/passwords



Personal example

17 physical authentication tokens:





Personal example (part 2)

22

- 10 pin numbers (bank, phone services)
- 3 personal computer passwords
- 6 server passwords
- 8 serious internet site passwords
- Too many non serious passwords to count.....mostly duplicates of each other

Probably in excess of 50 passwords!



Users: coping mechanisms

No coping mechanism for physical authentication.....

Virtual tokens:

- Common passwords
- Simple passwords
- Personal-information
- Management tools
 - Browser-saved passwords



Examples of common passwords

12345

abc123

password

passwd

123456

newpass

Notused

god

Hockey

internet

Maddock

12345678

newuser

computer

Internet

beer



Enter registered user details below

Email Address:

Password:

It doesn't matter if you use capital letters or not.

» [Log in to your account](#)

[Forgotten password](#)

[Change password](#)



Heavily used



Administering a password system

Easy to setup, the pain comes later once people use it:

Technical pain

- Securing the system
- Backing up the system
- Clustering the system
- Administering the system



Administrative pain

- Adding new users
- Expiring old users
- Changing passwords
- Distributing passwords
- Ensuring “proper” passwords used



Real world example





Real World example





Real World example





Summary

- User are overloaded with authentication tokens already
- There is explosive growth in the use of username and passwords
- Administering usernames and passwords is painful and expensive.



Break for coffee

Coffee being served outside

Back in 15 mins

On return Jon will talk about shibboleth



Shibboleth



What you need to know about shibboleth

- How it works
- What attributes are
- How federations work
- Your Identity stays at home
- Privacy sensitive by default



The core concepts of shib

- A user is authenticated at “home”
- Home knows who and what a user is
- Service providers make access decision based on what a user is
- Service providers should only know the minimum about a user



Core concepts of shib (technical)

- User redirected to home to authenticate and redirected back once authenticated.
- Authorisation is based on attribute description of a user sent between the two servers in the background
- Federations are used to group together service providers and institutes who can agree to the same rules

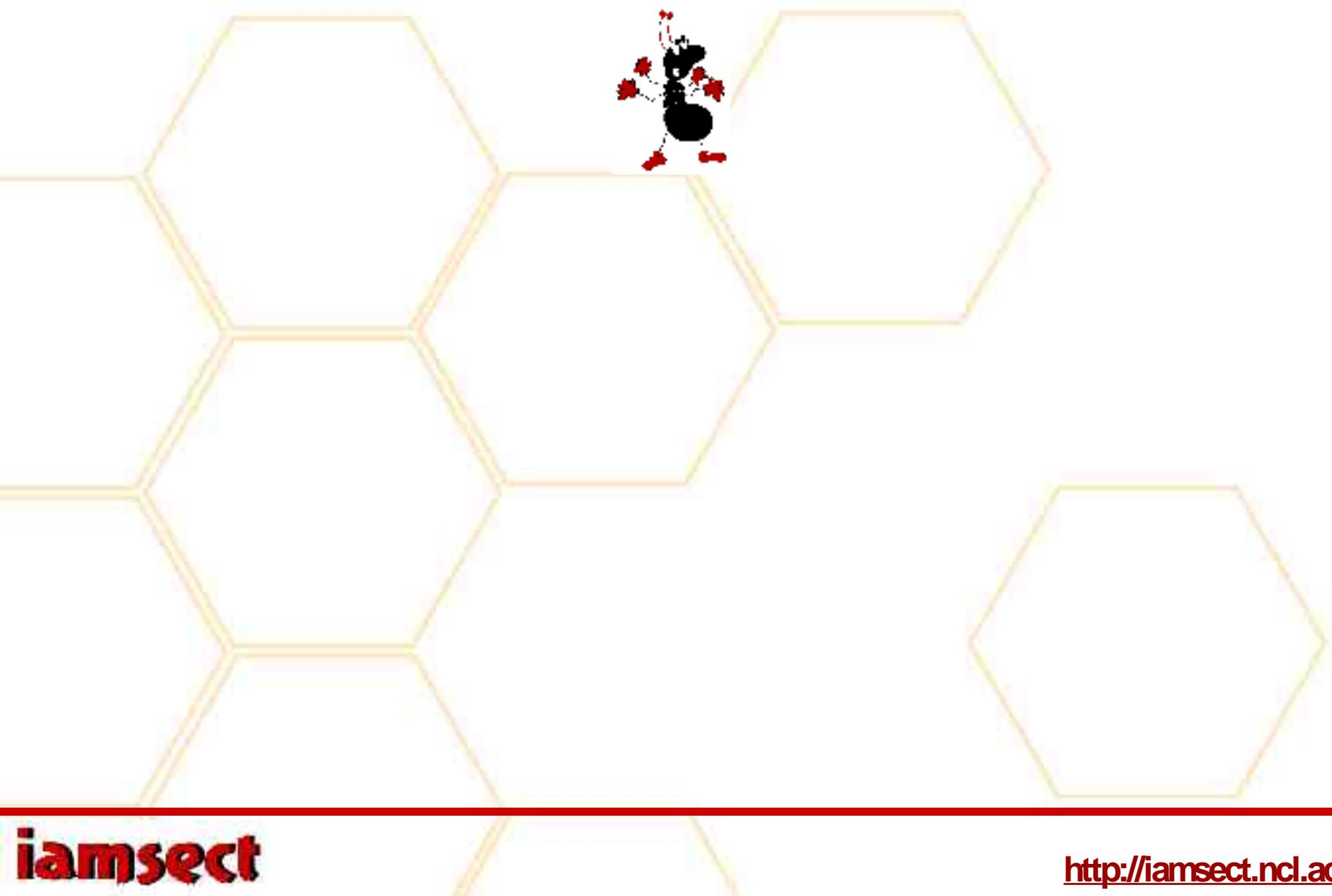


Demonstration (theoretical)

- At present, theoretical
- Durham Blackboard (Service Provider)
- Newcastle login (Identity Provider)

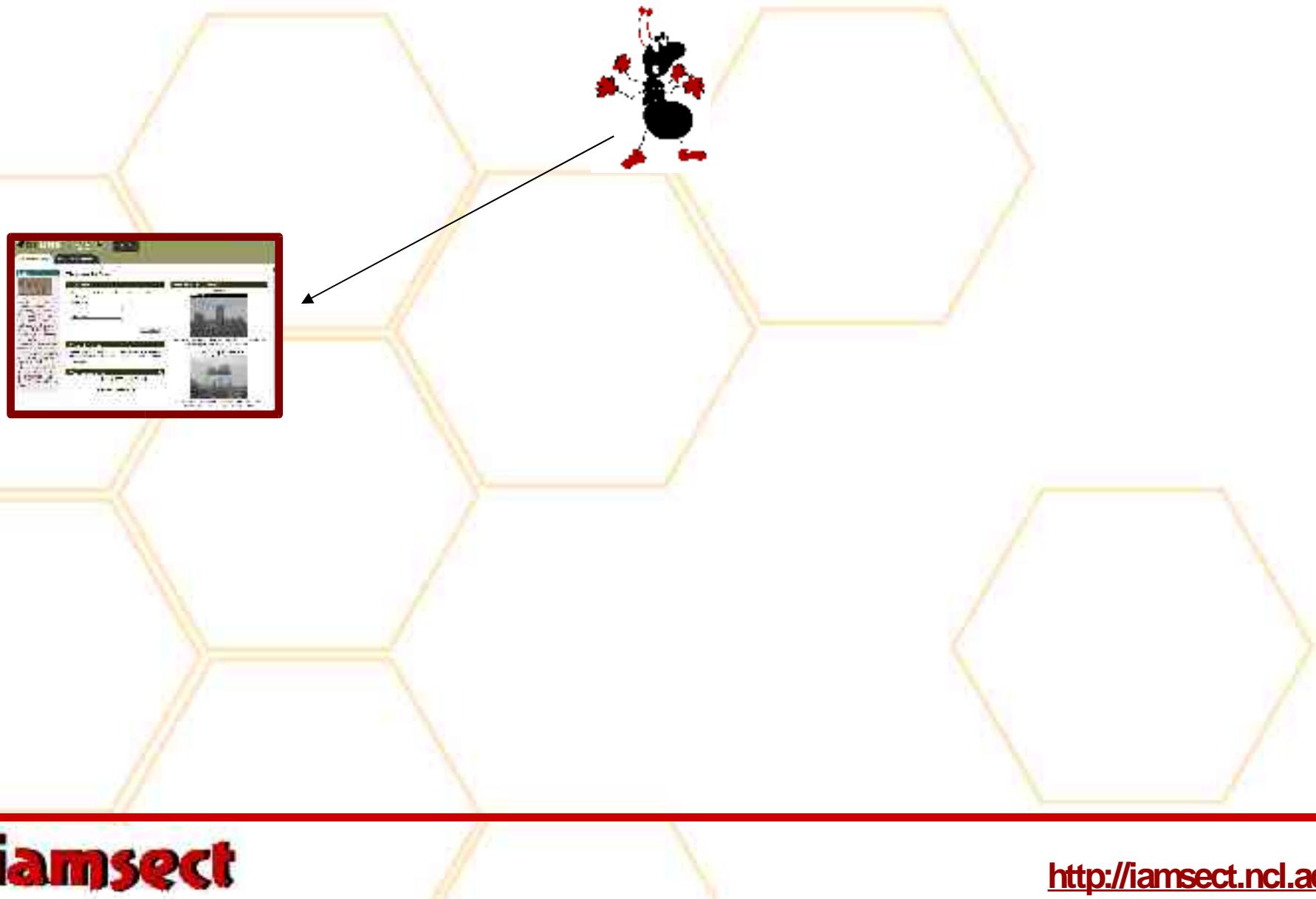


Demonstration





User attempts to access Service





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

Welcome to Bruno

1AMSECT Project Info

Links

duo

You are looking at Bruno - one of the University of Durham's Blackboard™ servers. Blackboard is the software which Durham uses to deliver the University's e-learning content. Bruno is a development server so such access is restricted and there's no much for guests to see. If you are interested in Durham's use of Blackboard™ the production server duo - Durham University Online

Welcome to Bruno

Login Here

What do you want? Every right information here can tell the registration below.

USER NAME:

PASSWORD:

Login

Acceptable Use

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

Usage for Mon 13/2/2006 15:52:51 EST

Total users in last minute: 1

Weather across Campus

Durham

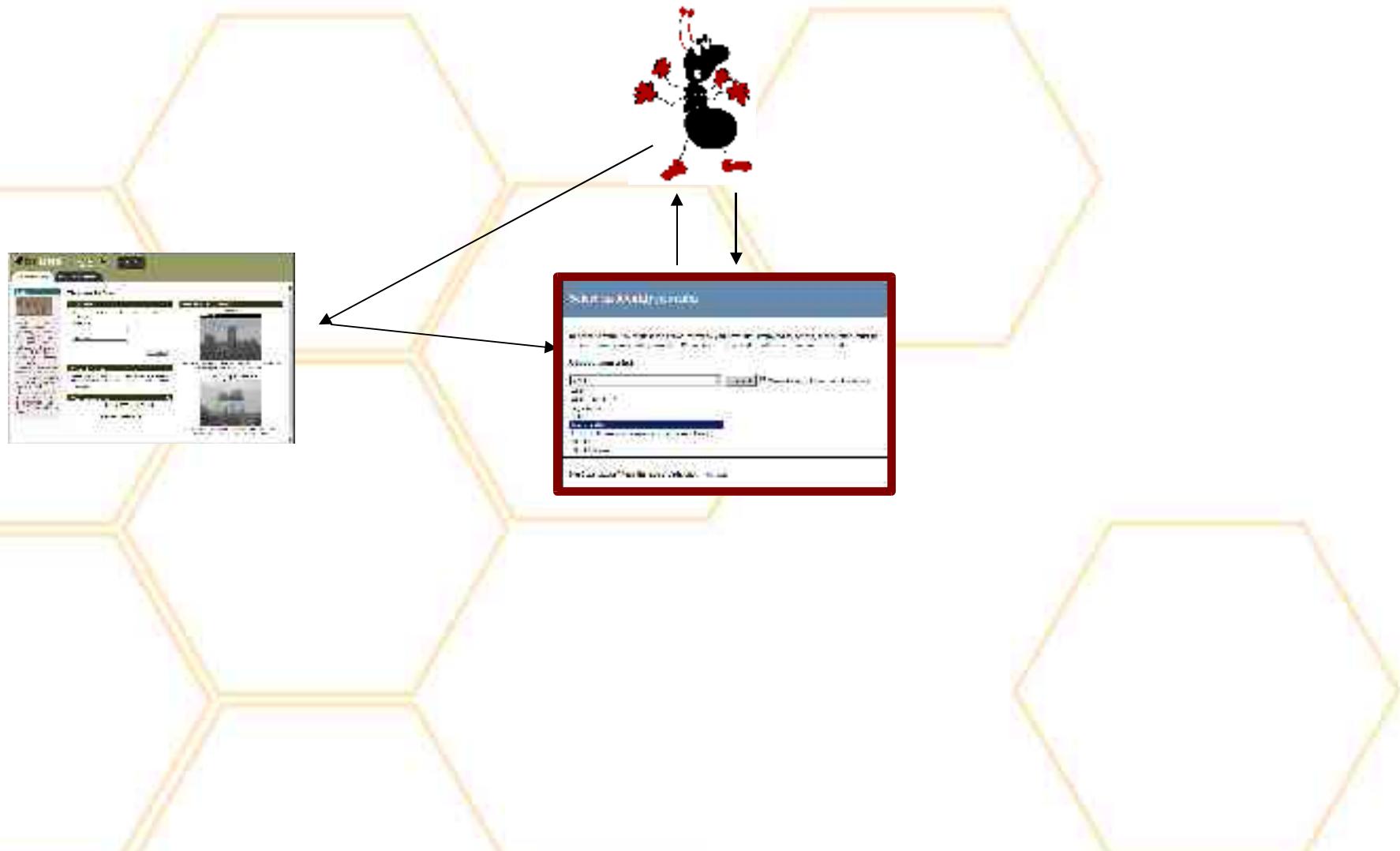
live image of Durham Cathedral from the Chetham's Armchair Webcam
Monday 13/2/2006 15:52:51 EST

Queen's Campus, Stockton

live image of the Transporter Bridge from the JBLI Webcam
Monday 13/2/2006 15:52:51 EST



User redirected to 'WAYF'





[https://wayf.sdss.ac.uk/shibboleth-wayf/...](https://wayf.sdss.ac.uk/shibboleth-wayf/)

Select an identity provider

In order to fulfill 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:

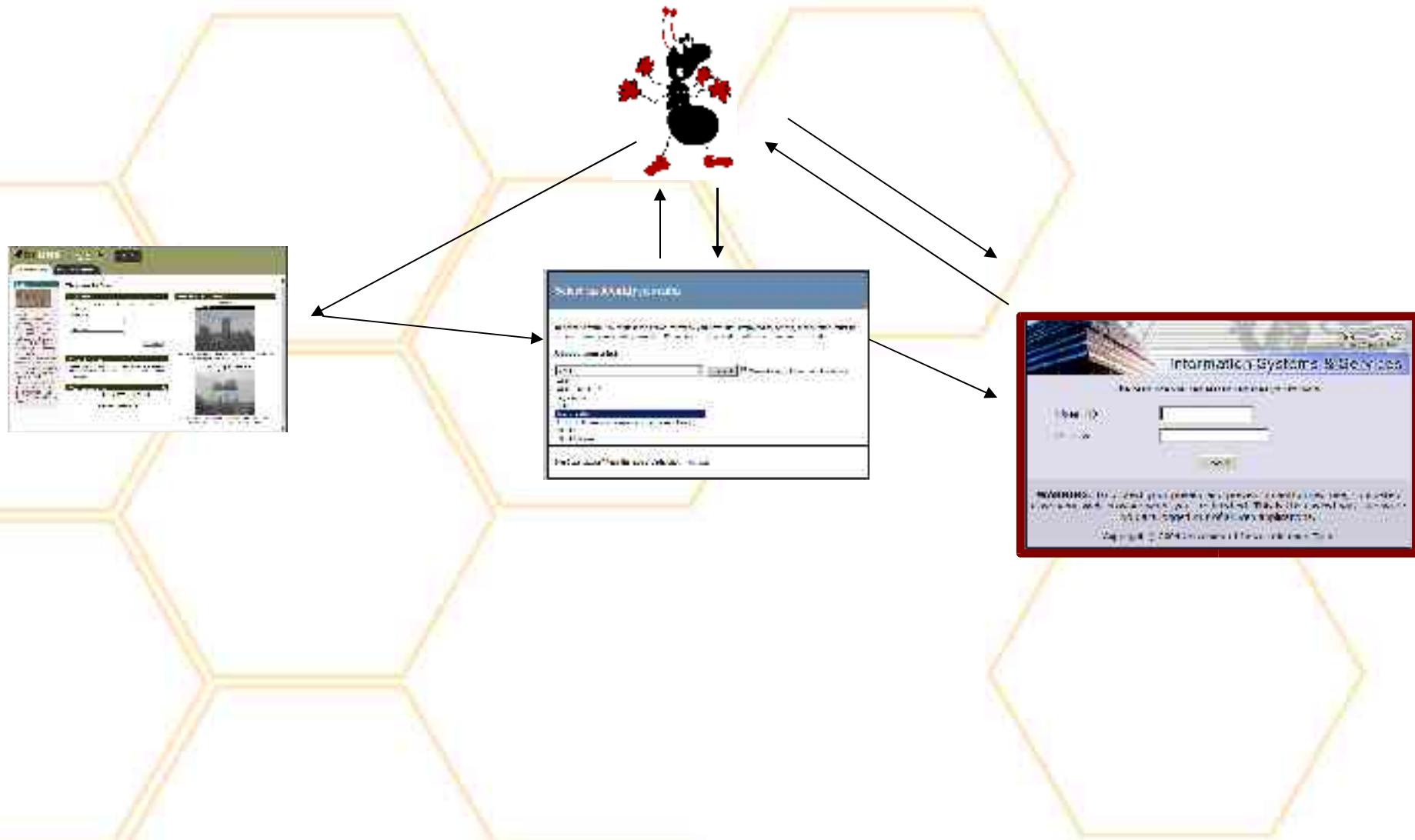
Remember my selection on this computer.

AMIE
AMIE_AUJTHZ
cy.org.uk
LSE
Newcastle
Oxford University Computing Services (Test)
SDSS
SDSS Newcastle

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

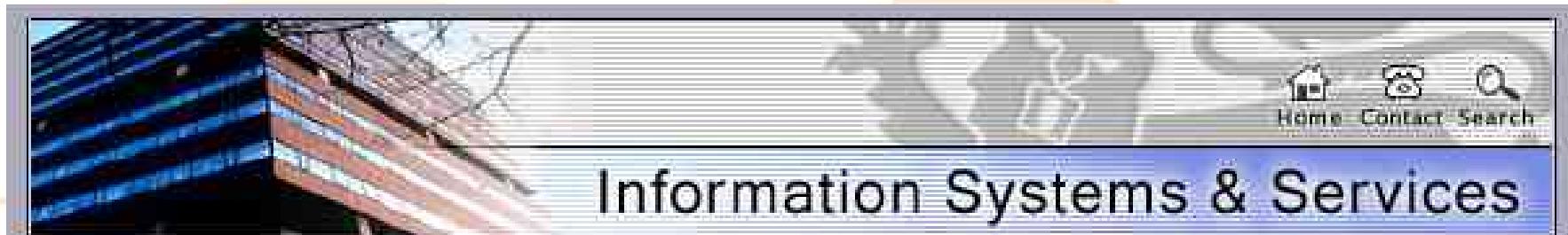


User selects their Identity Provider





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



Information Systems & Services

The resource you requested requires you to login.

User ID

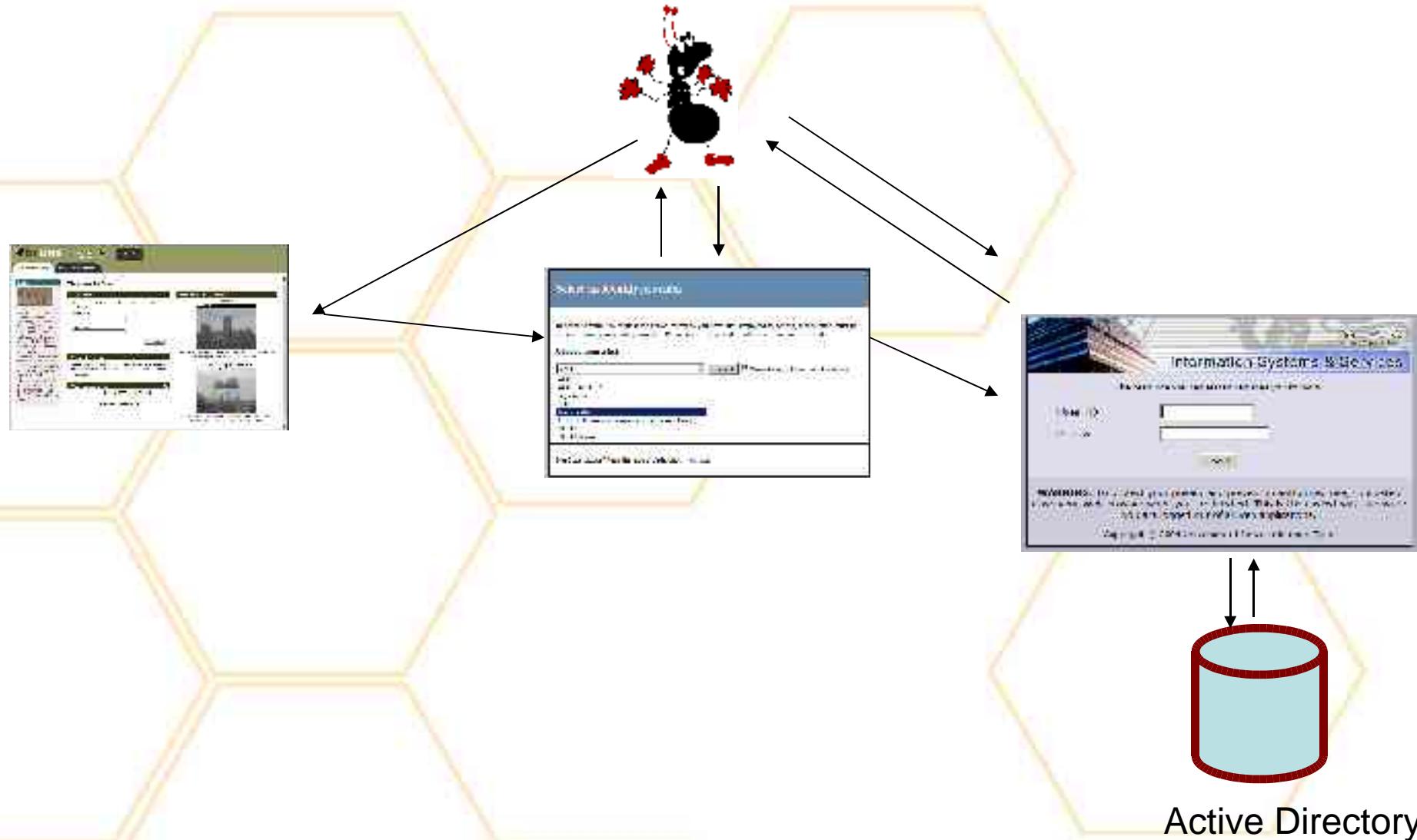
Password

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



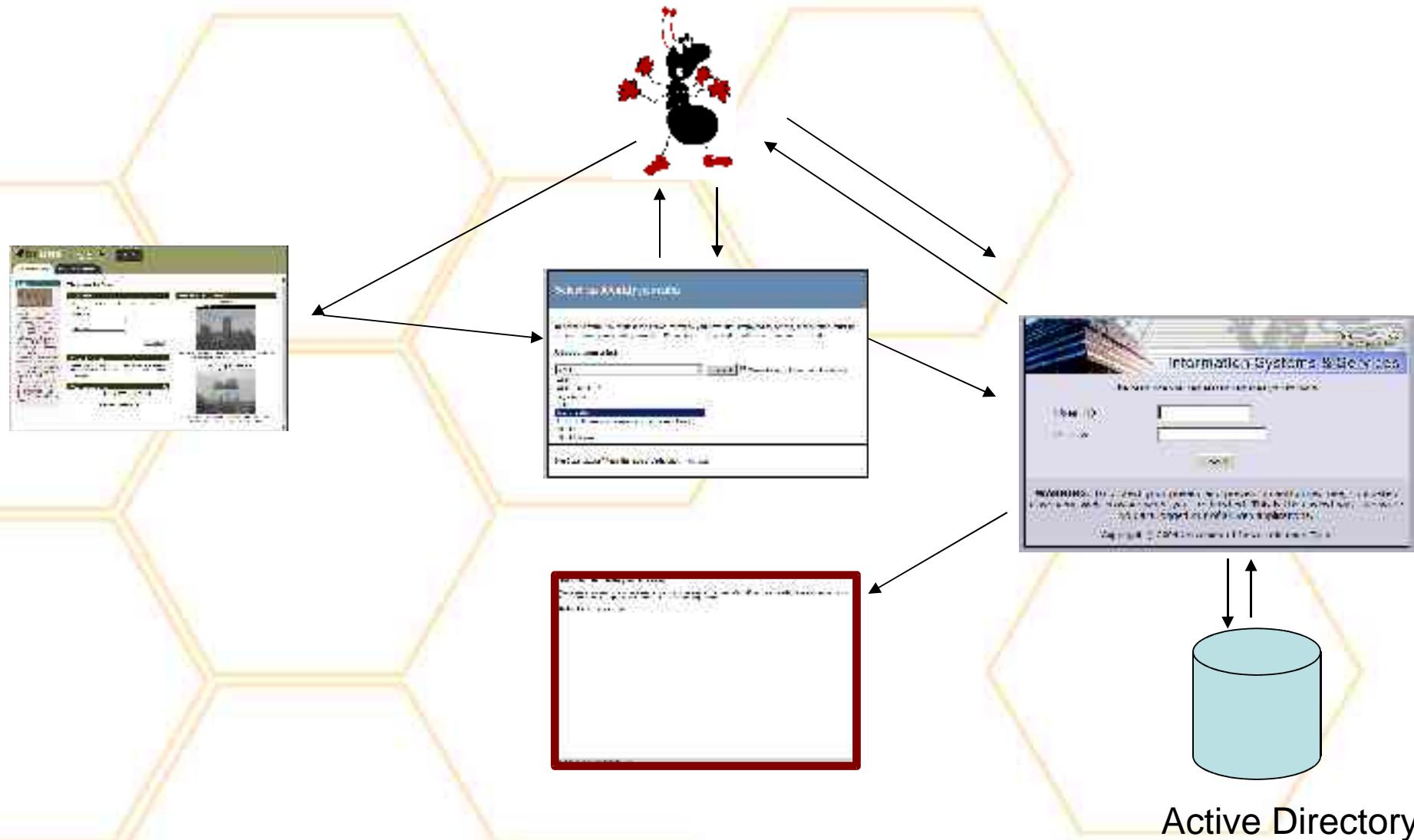
IdP authenticates User



Active Directory



User redirected back to Service





<https://shib.ncl.ac.uk/shibboleth/HS?...>

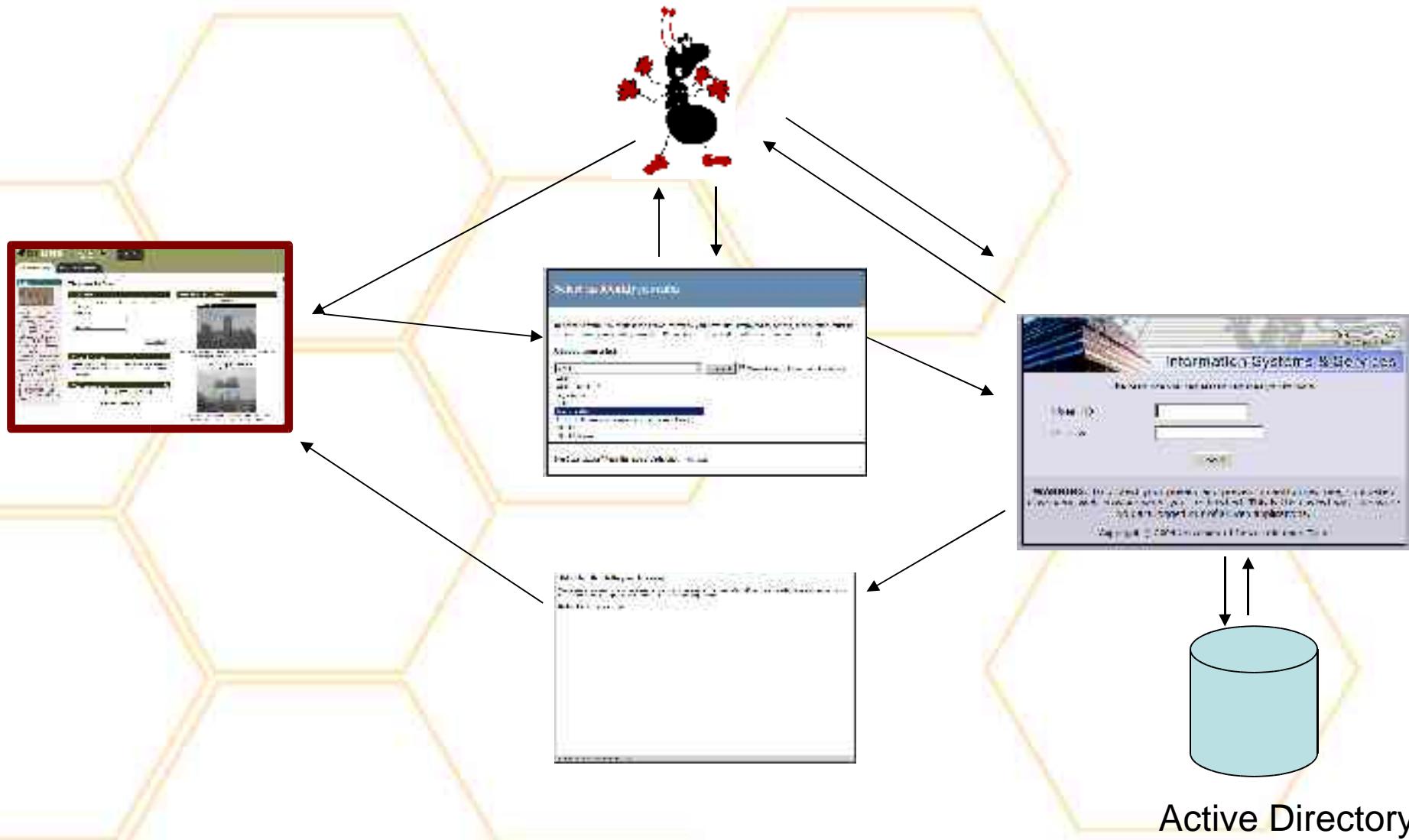
Shibboleth Handle Request Processed

You are automatically being redirected to the requested site. If the browser appears to be hung up after 15-20 seconds, try reloading the page before contacting the technical support staff in charge of the desired resource or service you are trying to access.

Redirecting to requested site...



User accesses Service





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

Screenshot of the Bruno LMS interface:

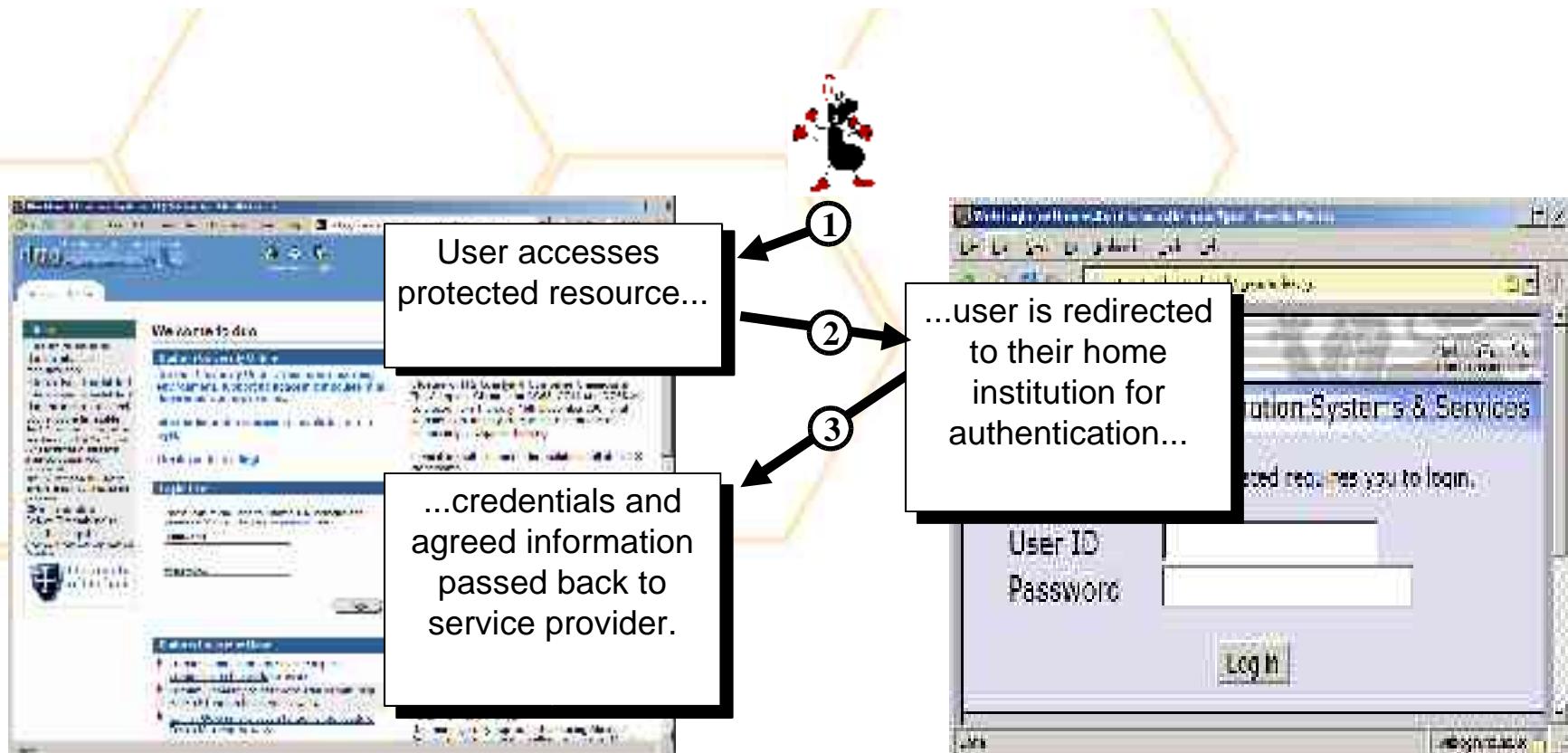
- Header:** Includes the Bruno logo, a navigation bar with Home, Help, Logout, and a Developer Copy button.
- Welcome Bar:** Shows Welcome, Courses, Community, Services, and a Tools menu.
- Tools Menu (Left):** Includes links for Announcements, Calendar, Tasks, View Grades, Send E-mail, User Directory, Address Book, and Personal Information.
- Welcome, Jon:** Personalized greeting for the user.
- My Announcements:** No system announcements have been posted today.
- My Courses:** You are not currently enrolled in any courses.
- Who's Online Module:** Usage for Mar 14 2001 12:21:27.673. Data: total users in last minute: 1, total users in last hour: 2.
- Your Source Institution:** UNIVERSITY OF NEWCASTLE UPON TYNE. This user is from Newcastle.



Demonstration (live)

- EDINA BIOSIS e-journal Service
- SDSS federation WAYF
- Newcastle Identity Provider

Shibboleth Process Simplified





Federations

- “Let us work together for unity and love.”

Mahatma Ghandi

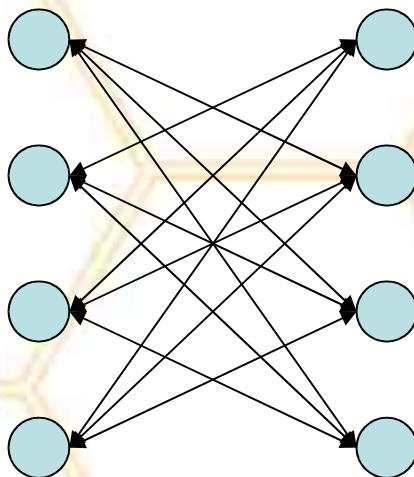


Federations

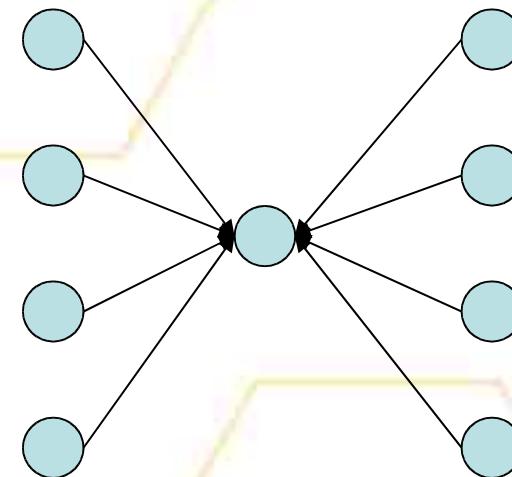
- Simplify the number of relationships
- Mutual policies
- Maintain WAYF server
- Technical requirements
 - Attribute standards
 - Certificate standards



Simplified relationships



24 relationships



8 relationships



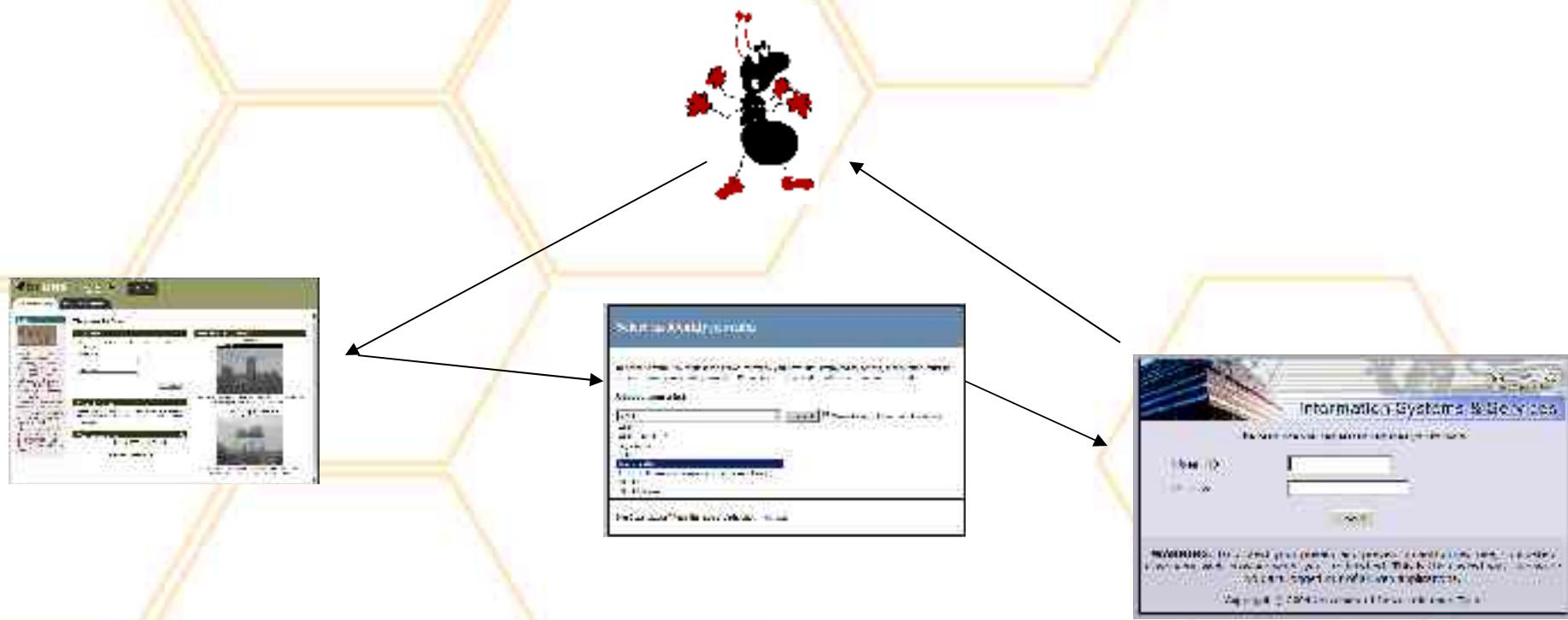
Federation Defined

- A grouping of identity providers and service providers following defined rules.
- More a social construct than a technical one.
- Components:
 - Participant agreement → trust others
 - Federation signup → data format agreement
 - Probable WAYF service....can be anywhere



Where are you from?

- Analogous to Athens DA Home Domain Discovery (HDD)
- Remember this relationship





Mutual Policies

- Federation membership may dictate abiding by a set of mutually agreed policies
- A common Certificate Authority (CA) for security



Example Federations

- InQueue
- InCommon
- Athens
- SDSS



SDSS Federation technical requirements

- Use Eduperson attributes:
eduPersonScopedAffiliation: *required*
eduPersonTargetedID: *optional*
eduPersonEntitlement: *contemplated*
- Use Globalsign as a certificate provider
moving away from this, they will be trailing
Thawte with newcastle.



SDSS Federation Policy V1.0

- All members of the federation must:
 - Observe best practice in the handling and use of your digital certificates and private keys
- All identity providers (origins) must:
 - Make reasonable attempts to ensure that only members of your institution are provided with credentials permitting authentication to your handle server, and that the assertions made to service providers by your attribute authority are correct.
- All service providers (targets) must:
 - Agree not to aggregate, or disclose to other parties, attributes supplied by identity providers.



Attribute Standards

- A common scheme for the exchange of attributes between service and identity providers



Baseline Rules

- Newcastle in the SDSS federation
- Newcastle currently BIOSIS subscriber but not UPDATE subscriber
- Can access BIOSIS via Shib, but not UPDATE



Attributes

- Descriptive information about a user
- Can technically be any descriptive text
e.g. has green eyes



How to identify useful attributes (theory)

- the attributes that are required by the web application;
- your institute's privacy policy;
- which attributes you can collect in a timely and scalable manner;



Identifying attribute (reality)

- Type and format will be decided by the federation you join
- Different Federations still likely to use the same standards
- You are not limited by federation, it is just there for convenience



Attribute identification (detail)

Current attribute use is limited to a dull but useful core

One major attribute standard in real use at present: EduPerson

One currently used attribute:
edupersonScopedAffiliation



eduPersonScopedAffiliation

- MACE-Dir eduPerson attribute
- Example: member@ed.ac.uk
- Gives subject's relationship to an institute
- At present can be one of:
member, student, employee, faculty, staff,
alum, affiliate.
- Many resources licensed on these terms
- “member” is all providers want to know for now



Attribute identification (detail)

Several more contemplated:

- eduPersonPrincipalName
- eduPersonTargetedID
- Given name
- Surname
- Common name
- eduPersonEntitlement



eduPersonEntitlement

- MACE-Dir eduPerson attribute
- Examples:
 - urn:mace:ac.uk:sdss.ac.uk:entitlement:resource
 - http://provider.co.uk/resource/contract.html
- states user's entitlement to a particular resource
- Service provider must trust identity provider to issue entitlement
- Good fine grained fall-back approach.



eduPersonTargetedID

- MACE-Dir eduPerson attribute
Example: sObw8cK@ncl.ac.uk
- A persistent user pseudonym, specific to a given service, intended to enable personal customisation
- Value is an uninformative but constant
- Allows personalisation and saved state without compromising privacy...much
- Issues about stored vs. generated forms



Attributes for the future

- Attributes are flexible so can be anything requires
- E.g. user on campus, “kiosk” walk in user, alumni.

Flip chart discussion



What is happening with shib now

Americans moving forward:

- Shibboleth being actively deployed
- 120 members with a test registration
- 13 Members already in their service federation
(\$700 upfront \$1000 per year)

Uk moving forward:

JISC £7m core middleware fund...more later

Athens infrastructure turbo charges UK shib



Athens services

ADITUS
 AMADEUS
 AMICO library
 APU Library Proxy
 Axiom
 BANKSCOPE
 BIDS CAB Abstracts
 BIDS IBSS Service
 BIDS Silver Platter INSPEC service
 BIDS SilverPlatter PsyclINFO 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 Update
 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 Aquatline
 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 KnowJK 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
 EEEBO
 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
 MIRAS 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
 Parlanet
 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



What is happening with shib now

Europeans:

2. Swiss switch project
3. Finns, Danes, Norwegians moving
4. Spanish, Germans seem keen

Australia:

Backing shibboleth after pilot studies



What is happening with shib now

Blackboard and WebCt actively integrating into their offerings
Elsevier deploying service
JSTOR service deployed
Athens integration
Anecdotal evidence that journal providers are very keen.



The future of shib

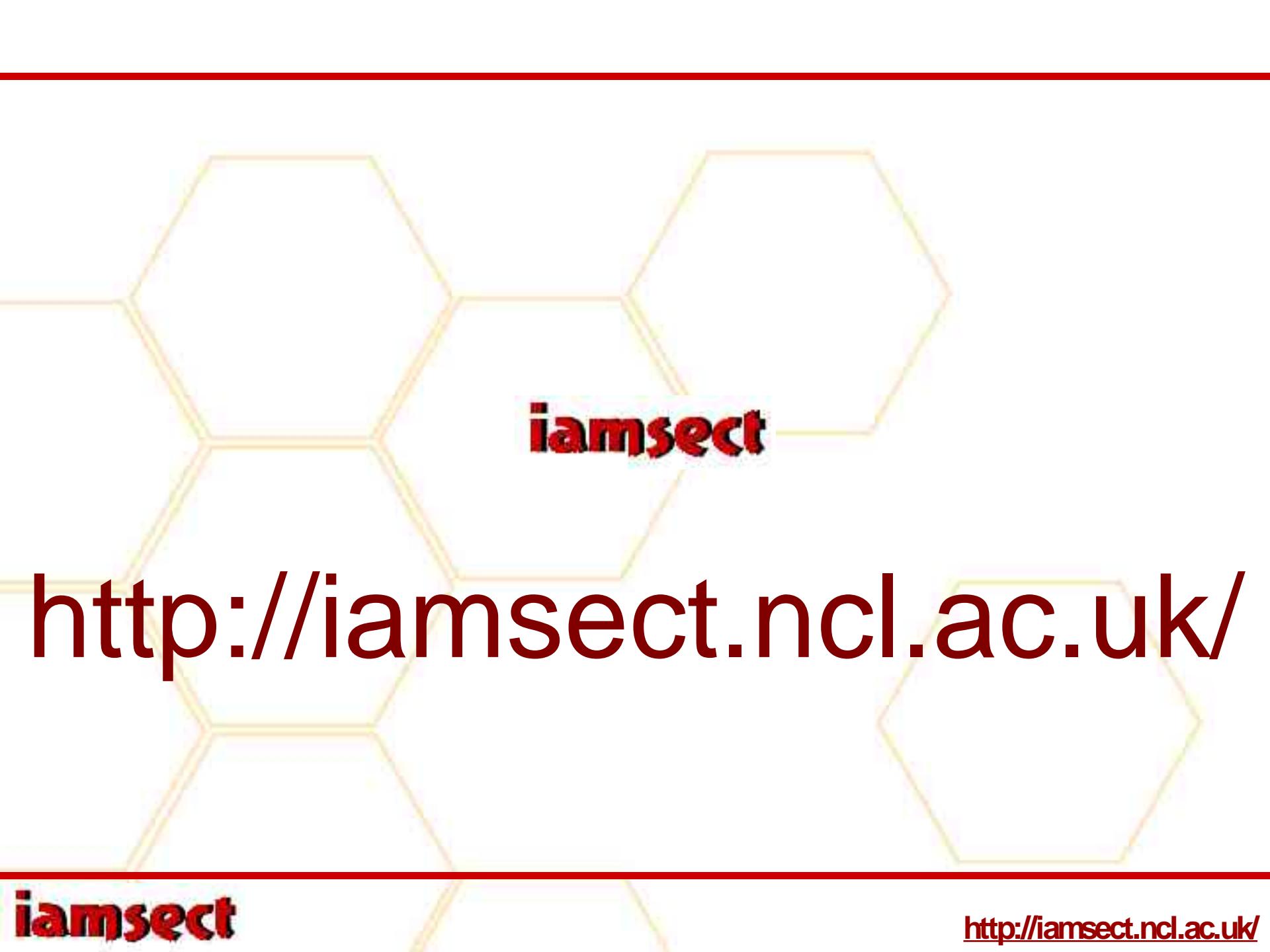
Shibboleth is a disruptive technology

Authentication, privacy barrier removed

- Online “reputation based” systems kill journals
- Services bought in from outside e.g. webmail for students
- Niche services flourish
- Desktop applications e.g. Lionshare



- “**I**nter-institutional **A**uthorisation
Management to **S**upport **e**Learning with
reference to **C**linical **T**eaching”
- JISC funded
 - Core Middleware Strand



iamsect

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



Inter-institutional

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



Other relationships

- SDSS
 - core middleware
 - EDINA
- SAPIR
 - early adopters
 - Newcastle University Library
- EPICS
 - regional e-learning
 - 5 Universities inc. us, 2 FE colleges



Authorisation, Clinical Teaching

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



Authorisation, Clinical Teaching

- Shared students

Medicine and Surgery (BSc) (Honours) UCAS Code: A106 (3 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

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?



Authorisation, Clinical Teaching

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



What we've done (1)

- Technical-oriented guides
 - Local SSO (pubcookie)
 - Shibboleth Origin



Guide to installing pubcookie

The screenshot shows a Microsoft Internet Explorer window with the following details:

- Title Bar:** Installing Pubcookie on Redhat AS 3.0 and authenticating against Windows Active Directory - Microsoft Internet Explorer
- Toolbar:** Back, Forward, Stop, Refresh, Home, Favorites, Help, and a search bar.
- Address Bar:** http://www.iamsect.ncl.ac.uk/~iamsect/installing-pubcookie.html
- Content Area:**

Installing Pubcookie on Redhat AS 3.0 and authenticating against Windows Active Directory

Table of Contents:

 - 1. Introduction**
 - 1.1. Purpose
 - 1.2. What is pubcookie
 - 1.3. Software required
 - 1.4. Environment required
 - 1.5. Assumptions
 - 1.6. Document Conventions
 - 2. Installation**
 - 2.1. Pre-requisites
 - 2.1.1. Remote File Systems (e.g. NFS)
 - 2.1.2. Accessing the Web
 - 2.2. Firewall settings
 - 2.3. NTP setup
 - 2.4. Apache Installation
 - 2.4.1. Getting pubcookie signed certificates
 - 2.5. Choose an Authentication Provider
 - 2.5.1. LDAP Authentication Provider
 - 2.5.2. Kerberos authentication provider
 - 2.6. Pubcookie Installation



Guide to installing shibboleth

The screenshot shows a Microsoft Internet Explorer browser window with the following content:

Installing Shibboleth on Redhat 5.1.1 using pbsocookie for authentication - Mozilla Firefox

File Edit View Bookmarks Tools Help

http://iamsect.ncl.ac.uk/section/1/docs/shib_start

1. Introduction

- 1.1 Purpose
- 1.2 What is Shibboleth
- 1.3 Skill Sets required
- 1.4 Equipment required
- 1.5 Assumptions
- 1.6 Document Conventions

2. Installation

- 2.1 Prior Configuration
 - 2.1.1 Remote File Systems (e.g. NFS)
 - 2.1.2 Accessing the Web
- 2.2 Firewall settings
- 2.3 NTP setup
- 2.4 Apache installation
 - 2.4.1 Getting proper signed certificates
- 2.5 Pbsocookie installation
 - 2.5.1 Installing the pbsocookie module
 - 2.5.2 Setting up the application server
- 2.6 Installing and configuring Java
- 2.7 Installing Apache Tomcat
 - 2.7.1 install the mod_jk2 connector
- 2.8 Installing shibboleth
 - 2.8.1 Secure the original conf file
 - 2.8.2 Setting up the Attribute authority configuration
 - 2.8.3 Join the impreme federation
 - 2.8.4 Use the real attributes



The guides

Written for redhat AS 3.0 linux:

- most popular
- will be supported for next 5 years
- Mostly applicable to other linux systems
- Cheap (\$60 per year...educational)

Content:

- Includes installation of all the required technologies for a shibboleth deployment
- Aimed solely at system administrators!

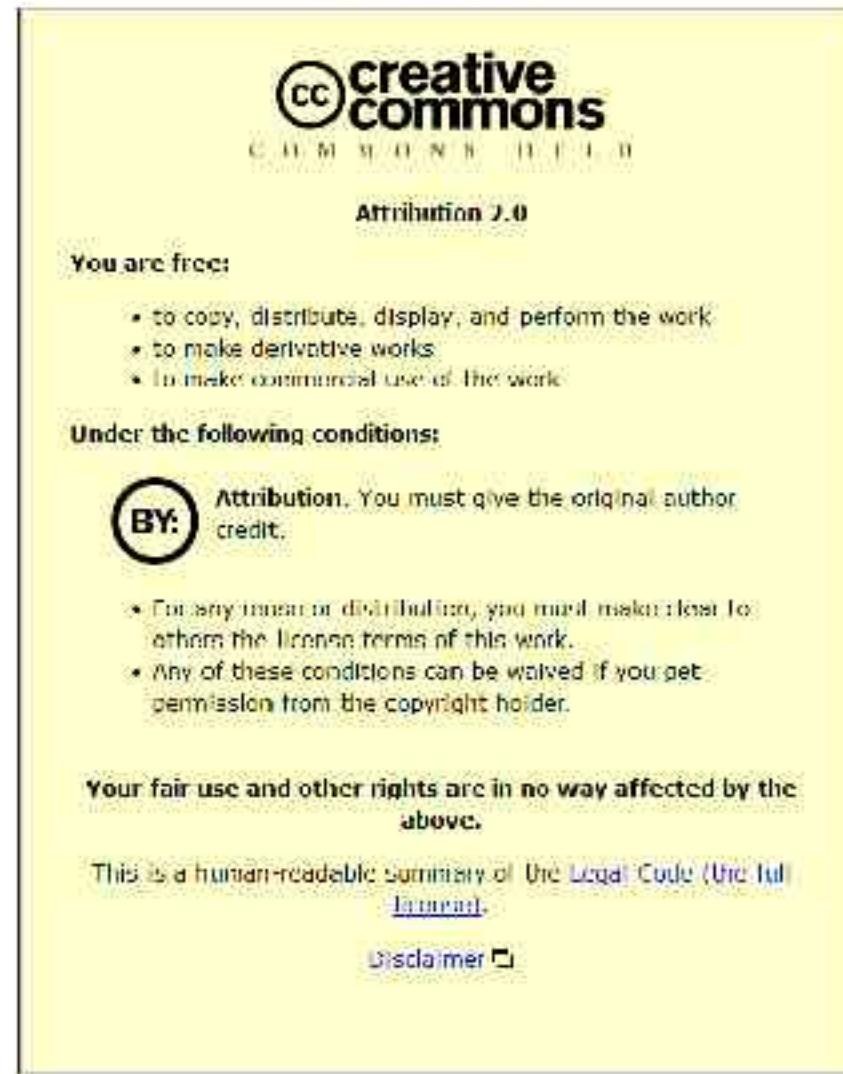


The guides

- Developed collaboratively
 - Written by Newcastle
 - Tested and proof-read by Durham
- Creative Commons
- In the process of hiring a technical author



Creative Commons



cc creative commons
C O M M O N S I N F O

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:

BY: 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 license).

[Disclaimer](#) 



Future guides

How to identify attributes attribute stores

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

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



The theory of our guides

- Endorsed by link from pubcookie site
- Possibly rolled into whatever the American's come up documentation wise for shib 1.3
- Looking for comments/feed back



What we've done (2)

- Shibboleth origin installation
- Shibboleth federation testing (SDSS)
- Glossary
- Questionnaire



iamsect

Glossary of Terms

Welcome to the IAMSECT glossary. This is designed to help people understand the terminology associated with Shibboleth, related technologies and the IAMSECT project.

You may also find the following glossaries useful: [EGLGlossary](#), [InCommon](#).

[RSS](#) [E-mail](#)

Index: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Active Directory

Microsoft's directory service product for storing user identity information, attributes and access policy. Active Directory is built into the Windows Server 2003 and the Windows 2000 Server operating systems.

Assertion



Questionnaire

- Determine 'baseline' opinions
- <http://iamsect.ncl.ac.uk/questionnaire/>



Questionnaire





A thought





What we're doing

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



How to prepare for shibboleth

Read the guides at:

<http://shibboleth.internet2.edu/shibboleth-doc>

Beware they are not user friendly

Mix managerial concerns with technical
concerns



How to prepare for shibboleth

Identify the following skill sets

Ability to:

Install secure ssl apache web servers

Install apache tomcat

Some familiarity with java

Familiarity with unix/linux

Technical staff to read the guides at

<http://iamsect.ncl.ac.uk/deliverables/>



How to prepare for shibboleth

Technical needs:

Identify password store or stores (how a federation can help)

Get a web sign on system (helped by our docs)

Identify attributes

Establish a certificate provider (Globalsign)



How to prepare for shibboleth

Identify federations you would like to join

Athens gateway

SDSS, EDINA federation

Establish a certificate provider (GlobalSign)

<http://www.ja.net/CERT/certificates/>