Web based single sign on

Caleb Racey
Web development officer
Webteam, customer services, ISS

Overview

- The need for single sign on (SSO)
  - User and admin perspectives
- Current state off SSO provision
  - pubcookie
- The future of SSO
  - shibboleth
- Preparing for the future

The need for web SSO

Proliferation of web based systems

- VLEs (Blackboard, Zope, NESS)
- Library catalogues
- Webmail
- Print credit purchase
- ePortfolios
- RAS….ish
- eJournals and eResources

- etc etc

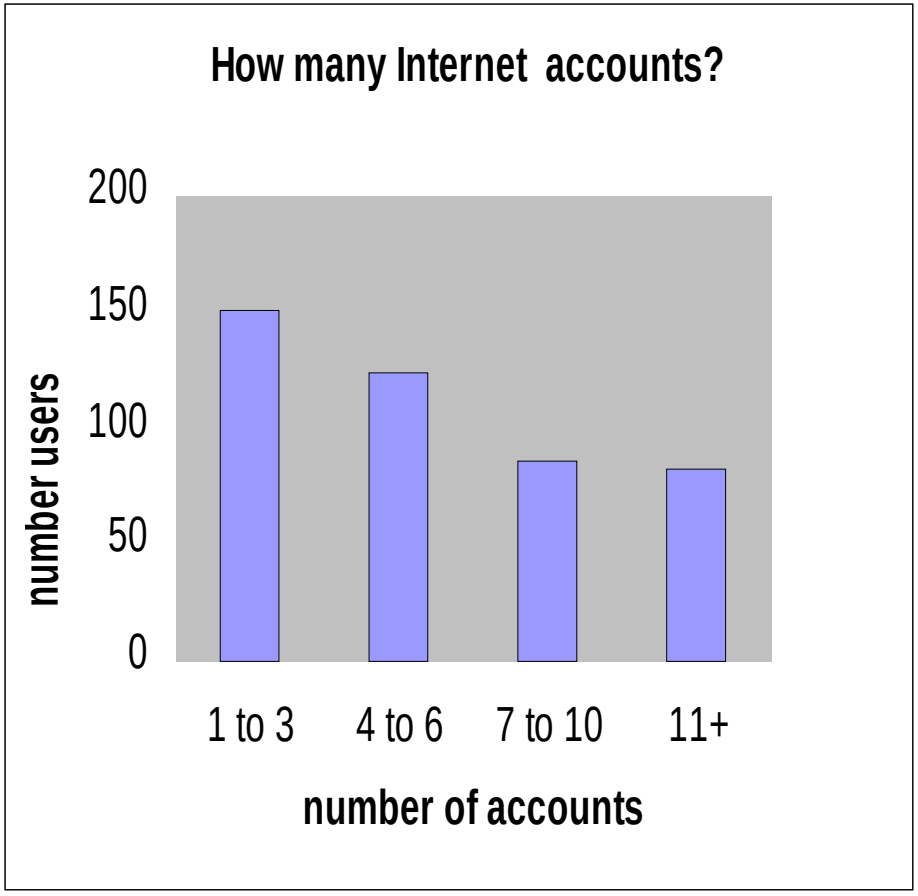
The need for web SSO

Proliferation of password stores
- ISS login
- Library login
- ePortfolios login
- Athens

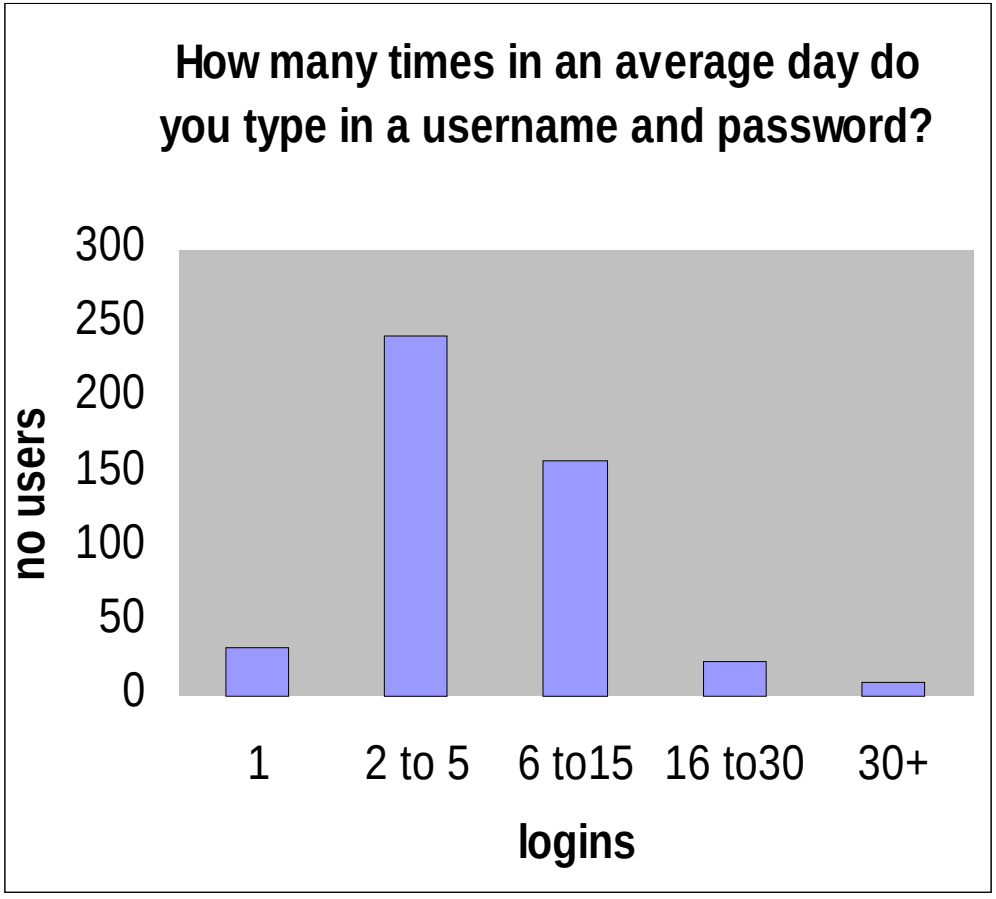
Lack of integration
- one username and password but many logins

Users and administrators overburdened

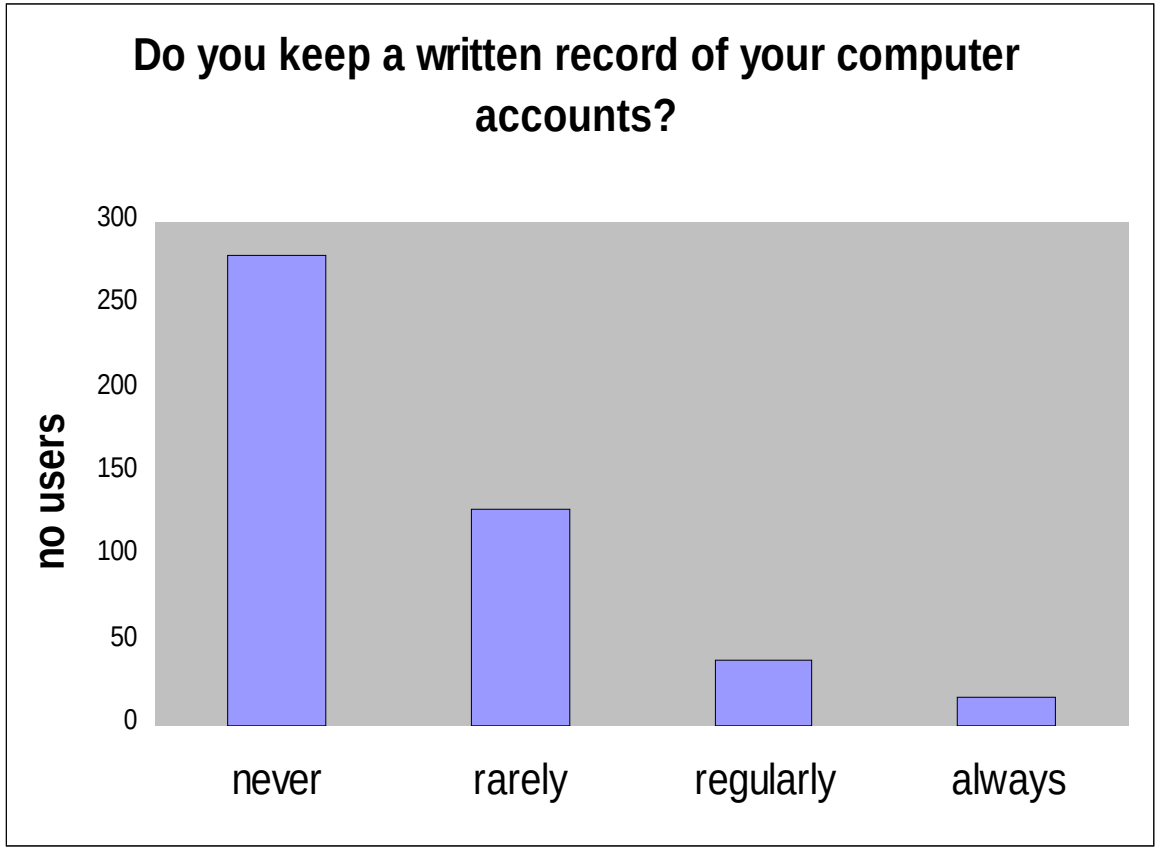
Users overload, Survey says:



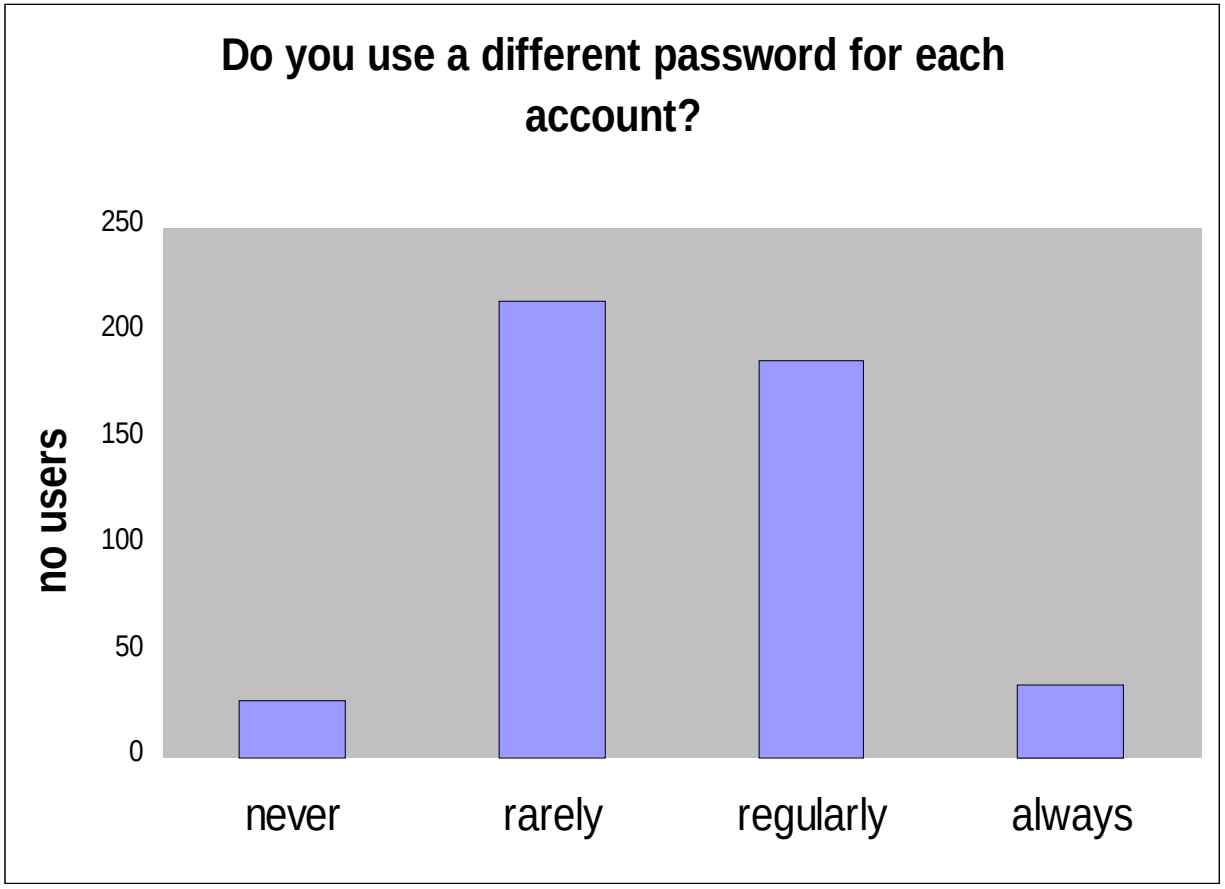
Users overload, Survey says:



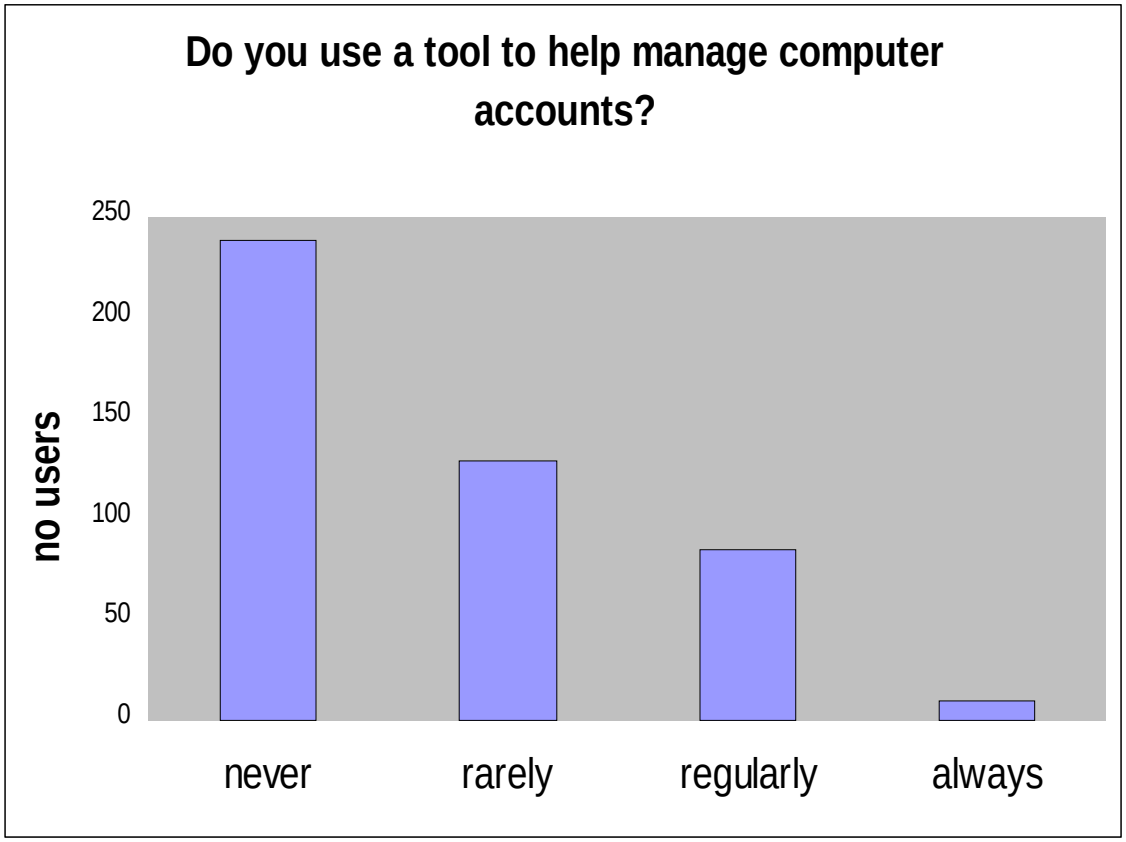
Users overload, Survey says:



Users overload, Survey says:



Users overload, Survey says:



Summary of survey

Users overloaded with different password stores and overloaded with login prompts

Half are using best practise with passwords

Half are not!

Current web username and password provision needs improvement.

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

Administering a password system

Management 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.

The Solution

One university password store:

- One password to remember
- One set of admins
- One education effort

Use pre-existing Campus username and password
stable, robust well resourced

For the Web

Pubcookie and Shibboleth

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

Pubcookie

Pubcookie

- In use for 2+ years
- Stable resilient infrastructure
- Apache and Microsoft IIS
- Can use LDAP or Kerberos to authenticate

Used by

Exam papers, Spam settings, Print credits

How pubcookie works

“Kerberos with cookies”

3) User tries to access protected application
4) Redirects user to login server
5) Authenticates against the Active Directory.
6) Redirects back to application with username in an encrypted cookie.

Pubcookie problems

Authenticates a user, limited authorisation
  burden on application developer
Clunky when used outside apache or IIS
  Python: zope, plone
  Java: tomcat, JBoss, websphere

Only usable internally,
Currently used in applications where role based authorisation not required
Managerially authorisation doesn’t scale

Shibboleth

Why the daft name?

Shibboleth: *And the Gileadites seized the passages of the Jordan before the Ephraimites; and it was so, that when those Ephraimites who had escaped said, "Let me go over," that the men of Gilead said unto him, "Art thou an Ephraimite?" If he said, "Nay," 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 the Jordan; and there fell at that time of the Ephraimites forty and two thousand.* (Judges 12:5-6, King James Version of the Bible)

i.e. The first recorded use of a password

Shibboleth

Federated Single Sign on standard from American Unis via Internet2

Based on SAML (Security Assertion Markup Language)

Summary: Athens and Microsoft passport functionality combined with added privacy

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

Terminology

Identity provider (IdP): the password store e.g. ncl

Service provider (SP): The application owner e.g. ejournal

The core concepts of shib

- Usable for on and off campus resources
- 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

Builds on top of pre-existing sign on (pubcookie)

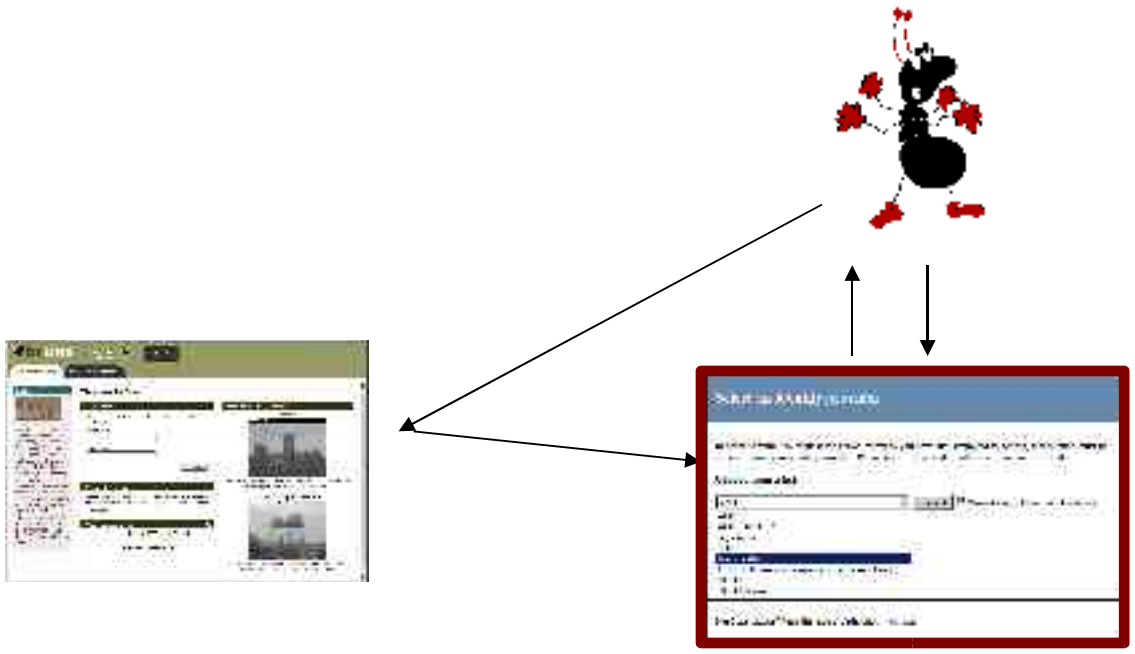
Core concepts of shib (technical)

- 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

What the user sees

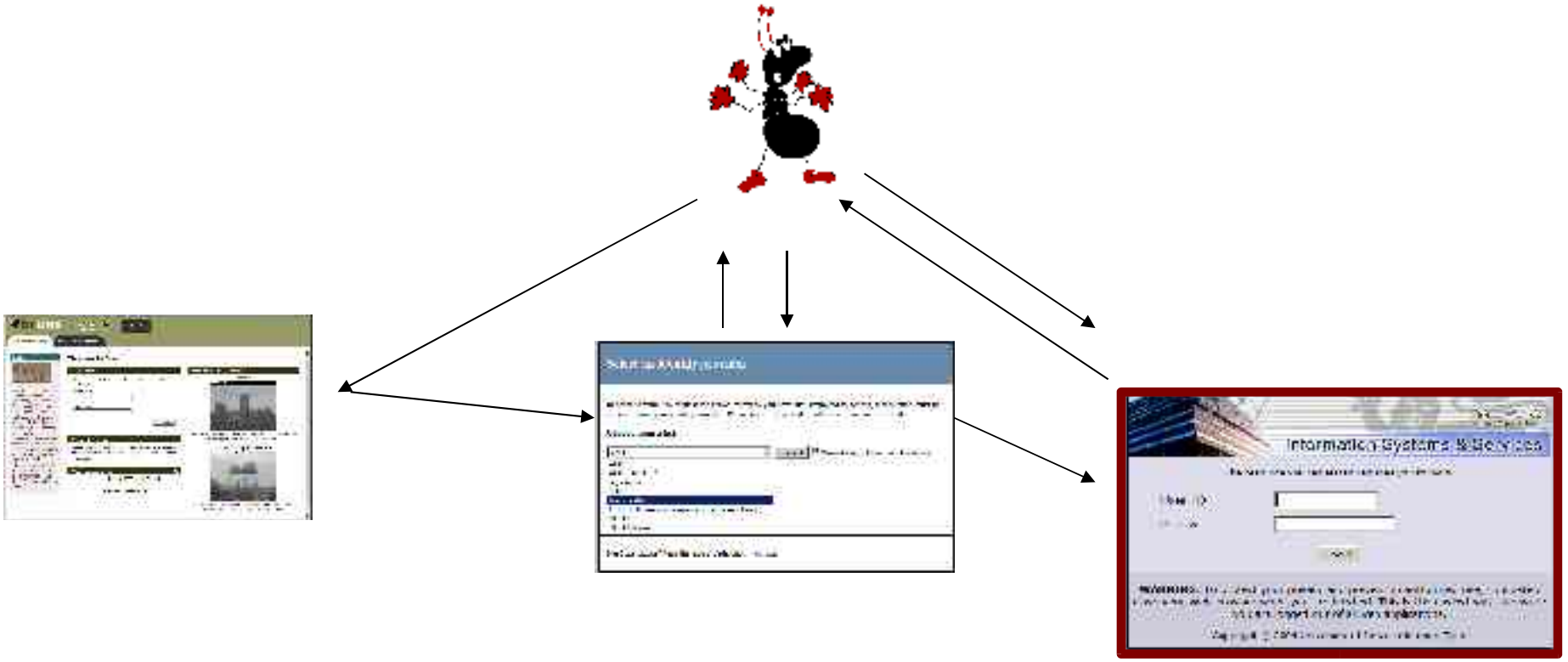
User attempts to access Service

User redirected to ‘WAYF’



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

User selects their Identity Provider



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

IdP authenticates User

User redirected back to Service

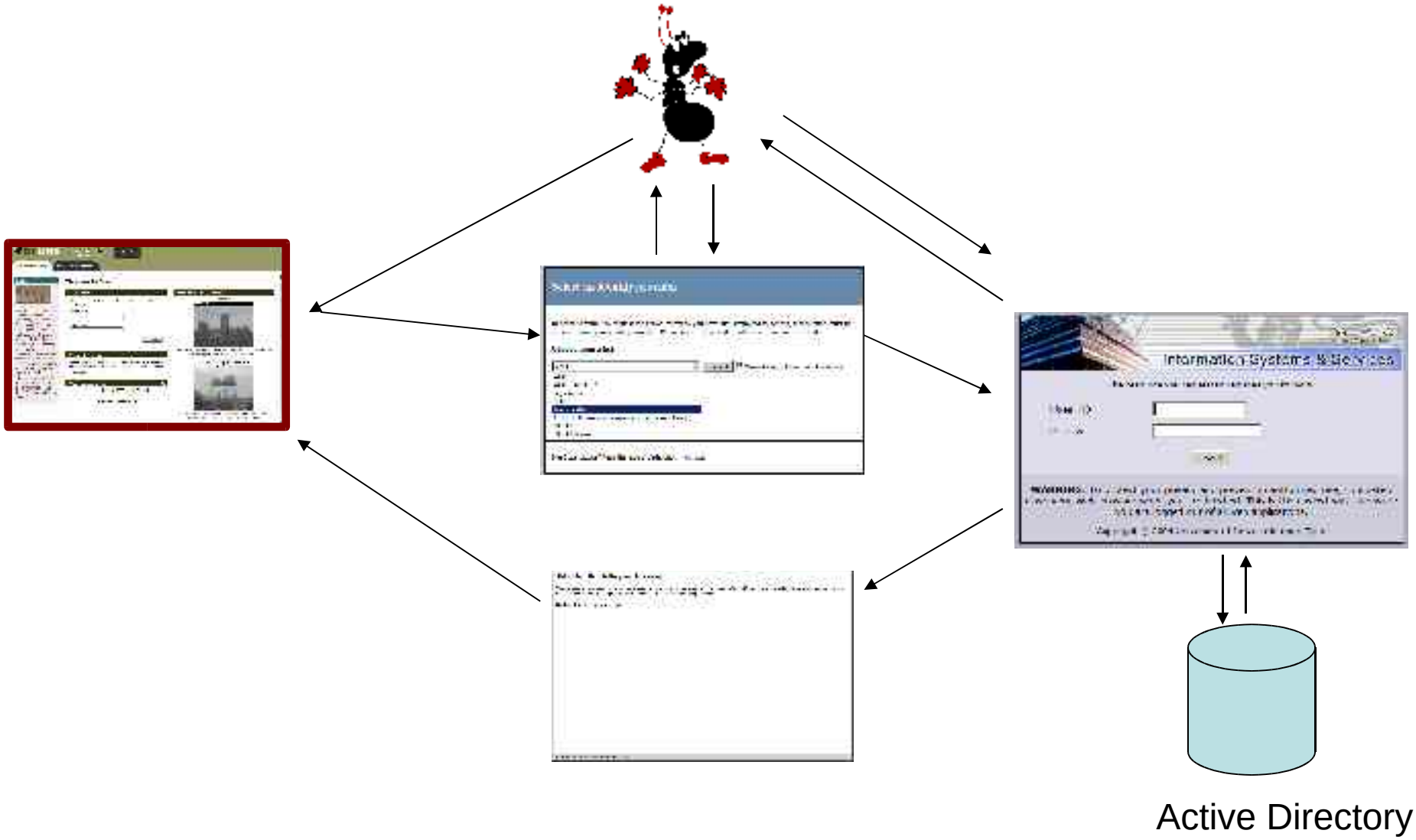
https://shib.ncl.ac.uk/shibboleth/HS?...

Shibboleth Handle Request Processed

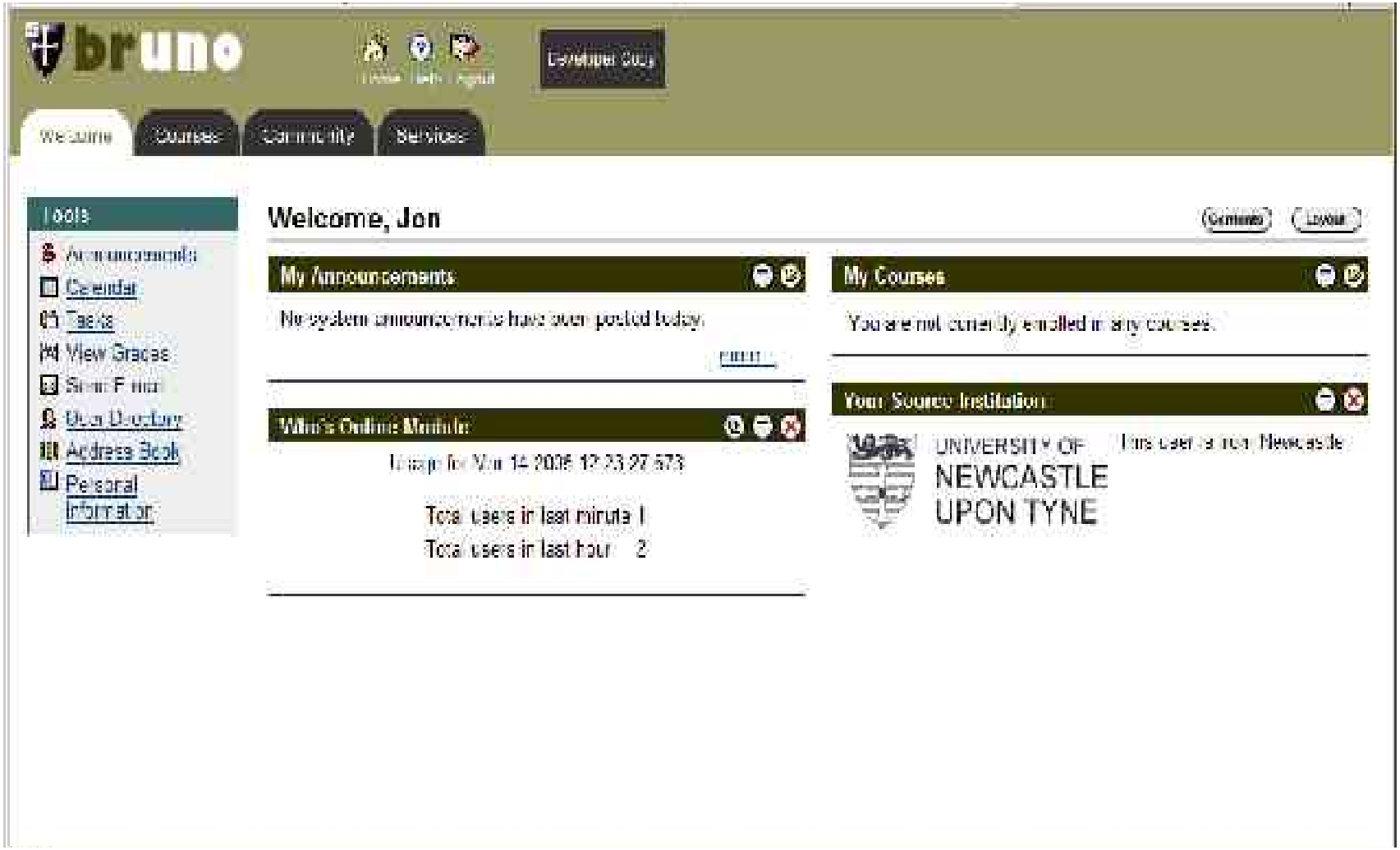
You are automatically being redirected to the requested site. If the browser appears to be hung up after 15-20 seconds, try reloading the page before contacting the technical support staff in charge of the desired resource or service you are trying to access.

Redirecting to requested site...

User accesses Service



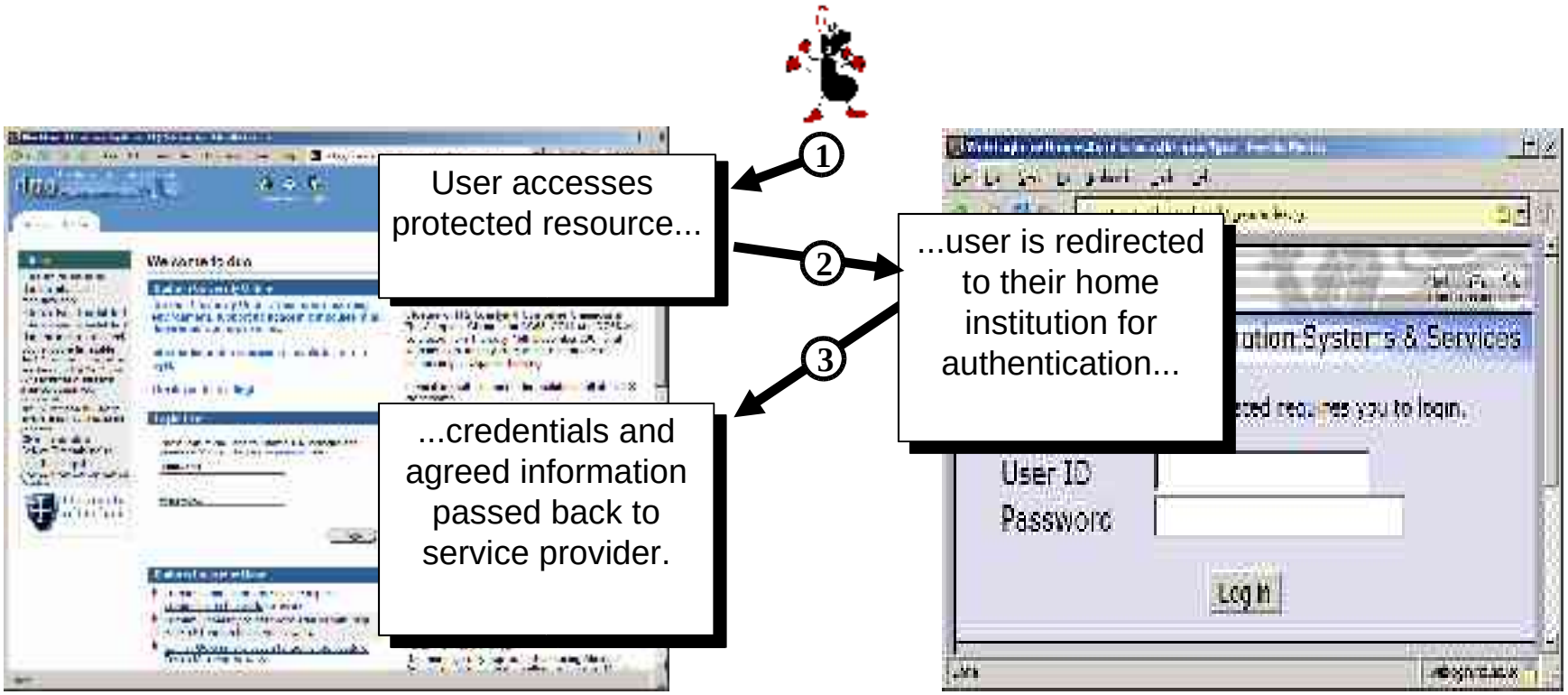
http://bruno.dur.ac.uk/



Demonstration (live)

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

Shibboleth Process Simplified

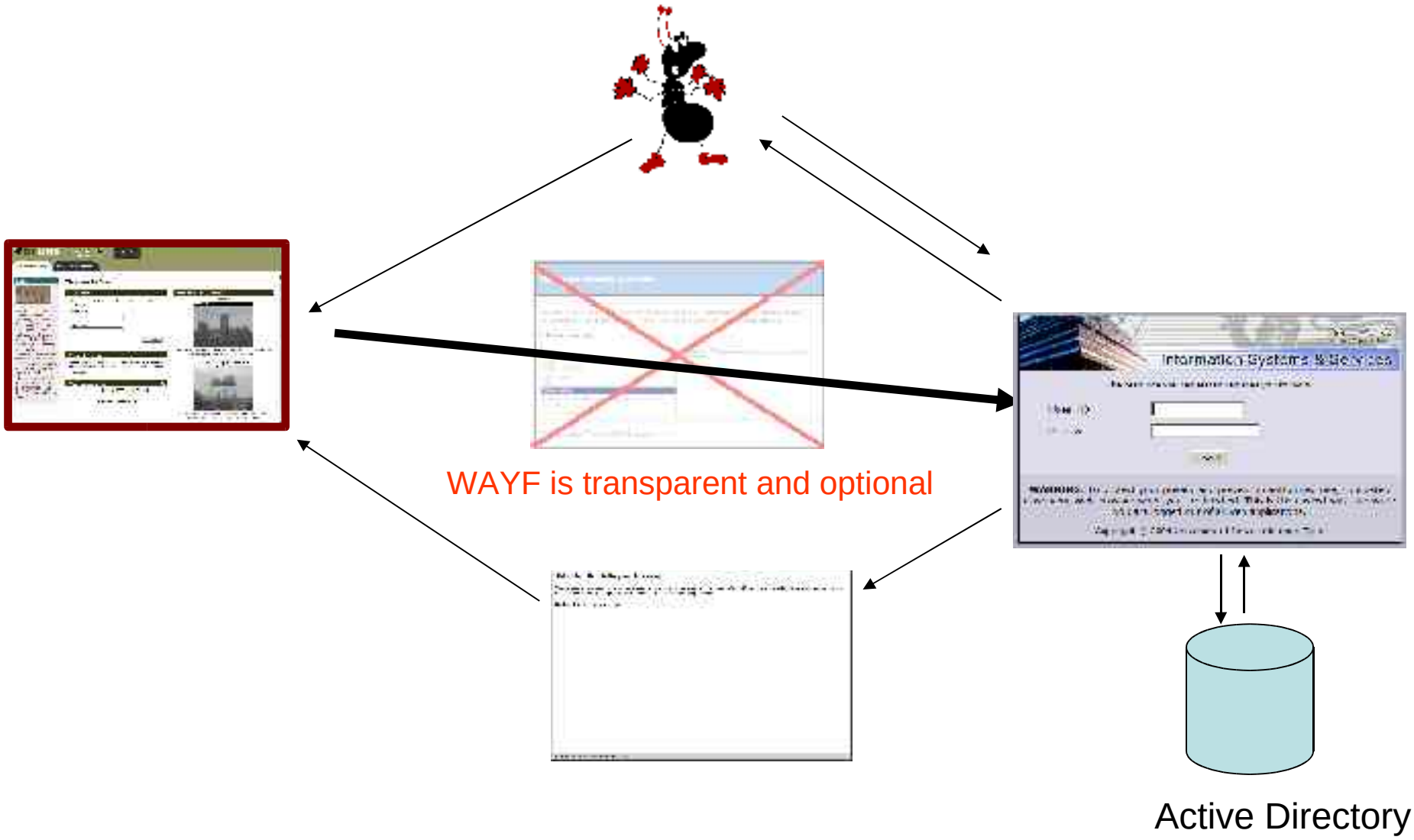


Benefits of shib

- Allows access control based on attributes i.e. enhanced authorisation
- Allows “secure” access control over http and https
- Prevents application developer from having to worry about login process

Usable internally and externally

Shib for internal apps



Attributes

Attributes are what shib uses to authorise.

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

Privacy sensitivities mean external attributes limited

Internal attributes not so limited

How to identify useful attributes (theory)

- the attributes that are required by the web application;
- your institutes 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)

For external consumption current attribute use is limited to a dull but useful core

One major attribute standard in real use at present: EduPerson

One current seriosly 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

eduPersonPrincipalName

MACE-Dir eduPerson attribute

Examples:

- *ncr18@ncl.ac.uk*, caleb.racey@ncl.ac.uk

- Equivalent to username
- Must be long lived and non recycled
- Must be unique

eduPersonEntitlement

- MACE-Dir eduPerson attribute
- Examples:
  - http://provider.co.uk/resource/contract.html
  - urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted
- 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 internal use

To be determined by the needs of application developers

e.g. users department, course, year of study, undergraduate or postgraduate, outstanding fines etc.

To be decided in consultation with you

Internal attributes (technical)

Need to be accessible in 3 seconds

LDAP or SQL querying

ideally consistent for different user groups, i.e. staff and student attributes are in the same place.

Advanced attributes

N-tier authentication

Potential to distribute “tokens” as attributes

e.g. NTLM or Kerberos tickets

Might be a solution to the n-tier problem

i.e. allow a portal to tell a user if they have new email without the portal having “read everything” permissions on mail store

Privacy sensitive

Attributes once aggregated are filtered twice:

- Site wide policy as to what to release to that service
- Overridden by User defined policy as to what can be released

Federations

Club of institutes agreeing to attribute formats and code of conduct

Organisational convenience, not technically necessary

Designed to cut down managerial overhead of having a relationship with many service providers

Why we are backing shibboleth

Many competeing standards: MS passport, liberty alliance, Ping identity

Shib has the momentum and drive in our sector

Shibboleth momentum worldwide

Actively Used in America, Switzerland, Finland

Australia, Hungary, Croatia actively deploying

Rest of Europe contemplating

American government looking at for governmental apps

Microsoft and Sun both interested in SAML/shibboleth, SAP SAML based, IBM interested.

SAML technical editor = Shib lead developer

Momentum UK

JISC funded core middle ware program
£7 million over next 3 years
£250k has come to Newcastle

BECTA has settled on shibboleth
NHS in early stages but interested

Athens will be fully Shib compatible by 2007

Shibboleth in Newcastle

IAMSECT project

JISC funded, collaboration with Durham and Northumbria

SAPIR project

Newcastle Library based

EPICS ePortfolios tag on

Life long learning portfolios transferable between NORMAN institutes

IAMSECT

Pilot study: federated access to resources between Durham and Newcastle

Medical students already shared

Shib enable

Durham blackboard

Newcastle Zope VLE

Newcastle Blackboard

Learn lessons with medics then role out for entire student population.

SAPIR

- Replace Athens with Shib
- Metalib portal Shib access
- Access to the Reading list management system.
- Aleph Library Management system access

Shibboleth Road Map

Immediate future

- trails with VLEs Blackboard, Zope
- Join Athens for journal access
- Library resources

Longer term

Investigate use with internal apps

Investigate buying in external service e.g. course submission software

Develop useful attribute set for internal use

Investigate in an N-tier context

Preparing for the future: what you need to do

Think about potential applications

Think about desirable attributes

Talk to us about needs and concerns

The future of SSO technology

SAML standard about to hit 2.0

Support for multifactor auth

Single sign out

Support for browserless apps e.g. Lionshare

Liberty alliance (Sun&co) Microsoft, SAP converging on SAML

The future of SSO community

Federated access control allows Unis to:

- buy in services: e.g. yahoo or google webmail
- sell services: course submission software, managed VLEs to higher education

Think of opportunities to sell services:

to Universities

to Schools

to NHS

to local government

to Industry

Summary

Federated single sign on a reality

Momentum is behind shib

We are in the driving seat in the U.K.

Genuinely disruptive technology:

- leads to opportunities.

Questions?

Caleb.racey@ncl.ac.uk

http://iamsect.ncl.ac.uk