



# Using Federated Access to restrict access to “Authorised Users” only

Dr Rhys Smith  
JANET(UK) & Cardiff University

# JANET(UK)



- JANET is the UK's education and research network
- Approximately 18M eligible end users within UK schools, FE/HE and ACL programmes
- JANET(UK) manages the operation and development of the JANET network on behalf of the JISC for the UK FE/HE Funding Councils
- Not-for-profit company operated as a public-sector organisation
- Core network plus additional services



# ERA plus

- ...which will enable licensed ERA Recordings to be accessed

*by students and teachers*

Errrr?

online whether they are on the premises of their school, college or university, or at home or working elsewhere

*within the UK*

GeoLocation

# Errrr? Continued



- ERA plus says:
  - “Licensees will be required to have in place procedures to ensure that only “Authorised Users” will be able to gain access to ERA Recordings stored on the servers of a licensed establishment.”
- So it’s up to *you* to enforce “Authorised Users” (students/teachers)
  - GULP!



So, the question is:

**how do you do that?**

**Well...**

# Déjà vu for Us...



- This problem is very common in the education sector
  - Access to subscription resources (e.g. academic journals) needs authenticated access, anywhere, anytime
  - Access to institutional resources (e.g. VLE, portal, timetable, etc) needs authenticated access, anywhere, anytime
  - Etc.

# ...is good fortune for you



- No need to reinvent the wheel
  - Reuse existing solutions
- So what are they?
- Main technology in use in education sector is Federated Identity

# Federated Identity/Access



- Federated access management (FAM)
  - one organisation asserting information about its users to another
- Many flavours of FAM
  - e.g. openID, Infocard, SAML, Facebook Connect
- SAML is widely deployed in education
  - Open standard, stable, secure, free to use, no vendor lock-in, etc.



# The UK federation

- SAML based Federated Identity Federation
- Launched November 2006
- For UK Schools, FE/HE and Research *and* Organisations and institutions providing services to these sectors
- N.B. ~40 national education/research federations worldwide



# Organisational structure

- Joint funded by Becta & JISC
- Operated by JANET(UK)
- Policy Board
  - Rules of Membership
- Technical Advisory Group
  - Technical Recommendations



# UK federation in a nutshell

- A collection of members
- A set of Rules that binds members:
  - Make accurate statements to other members
  - Keep federation systems and data secure
  - Use personal data correctly (DPA1998)
  - Resolve problems within the Federation
    - Not by legal action

# High level aims and objectives



- Provide a secure framework for gaining access to licensed content.
- Make it easier to comply with regulatory requirements such as DPA.
- Protect the privacy of the end user.
- Standards based and open source.

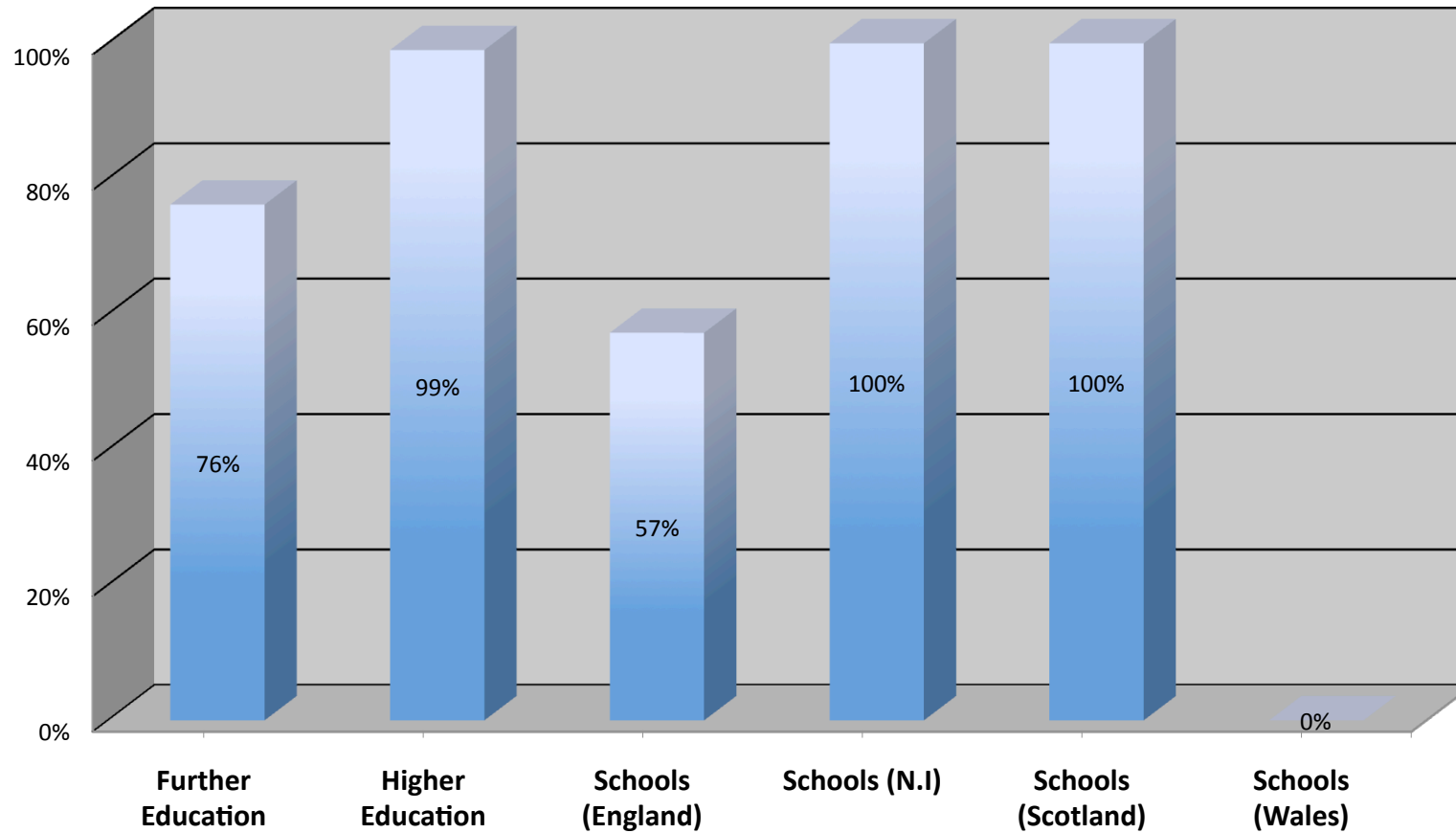
# UK Access Management Federation



- 826 members
  - 653 “Home Organisations”
  - 490 “Services”
- Cross education sector solution
  - Primary School -> University
  - And beyond?



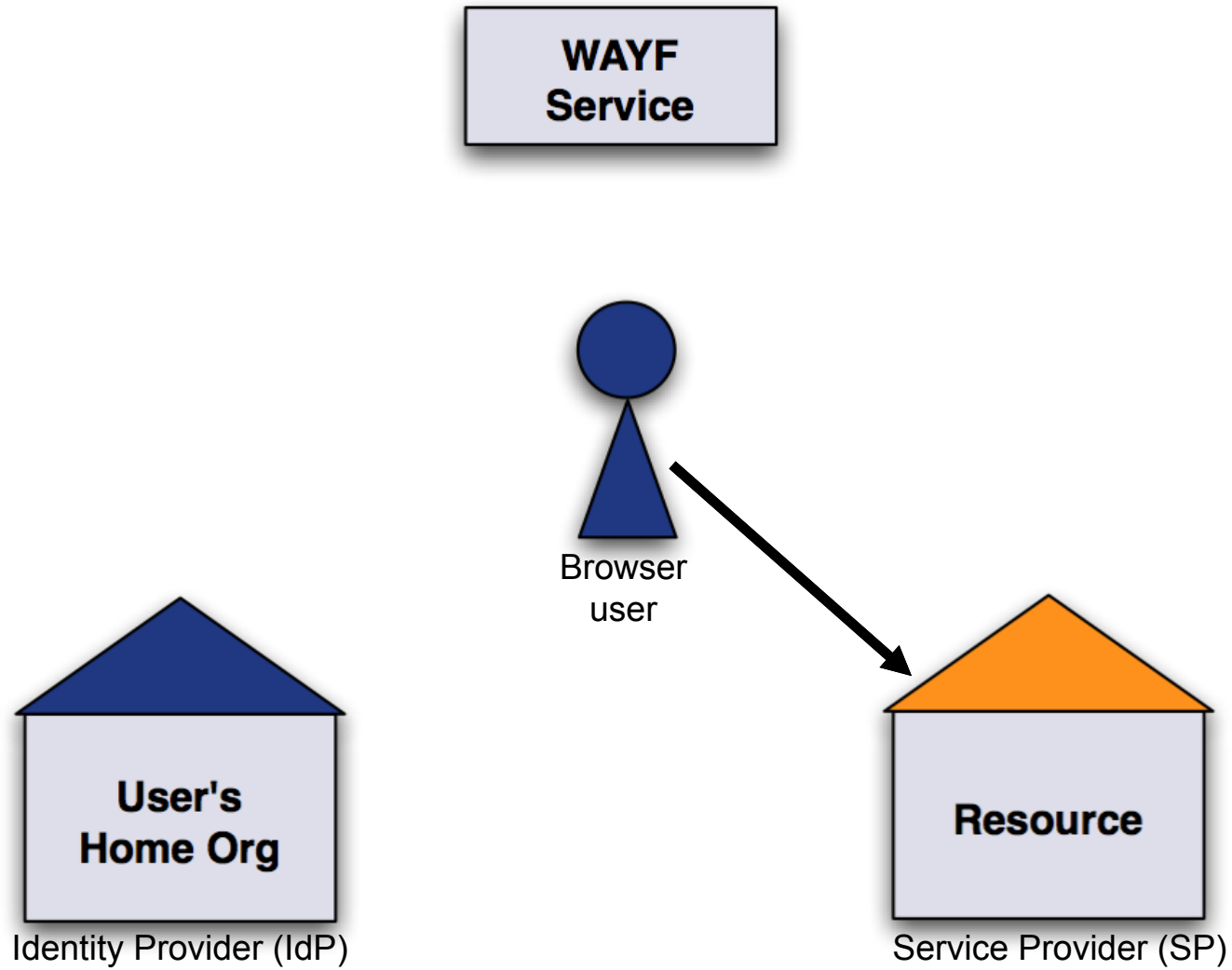
## Membership by Sector





- Shibboleth is an open source technology that enables federated access management, developed by the Internet2 Group. It both triggers the authentication process within an institution, and supports the secure exchange of information to establish authorisation.
- Shibboleth is an implementation of an open standard known as SAML (Security Assertion Mark-Up Language).
- Shibboleth is the recommended software for UK federation participation.

# How it works

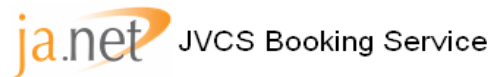


JVCS Booking Service - Mozilla Firefox

File Edit View History Bookmarks Tools Help


http://www.jvcs.ja.net/cgi-bin/vcng/welcome.cgi

BBC NEWS | News Front Page JVCS Booking Service



## JVCS Booking Service.

The JVCS Booking Service enables registered users to create videoconference booking requests and to view the details of videoconferencing facilities at any of the JANET registered organisations.

 **By accessing this service** you confirm that you have read and accepted the [JANET\(UK\) privacy policy](#) and will not share personal data of registered users of this service with any third party. You also confirm that you will not enter personal data of any kind in a title or additional information field of any videoconference booking.

In order to comply with the [Data Protection Act](#) it is not possible to browse for any details of booked videoconferences without first registering to use the service. To [register to use this service](#) you must be a member of staff of a JANET primary connected organisation. Note that registration is subject to approval and may take several days.

Registered users login here - [Register to use this service](#)

Email Address:

Password:

[Forgotten password?](#)

Login

Alternatively, [login](#) or [register](#) using Shibboleth. [Help on Shibboleth.](#)

The **JVCS Management Centre** is open Mon-Fri 08:00-21:00 & Sat 08:00-17:00 and can be contacted on +44 (0)131 650 4933 or by e-mail to [vidconf@jvcs.ja.net](mailto:vidconf@jvcs.ja.net).

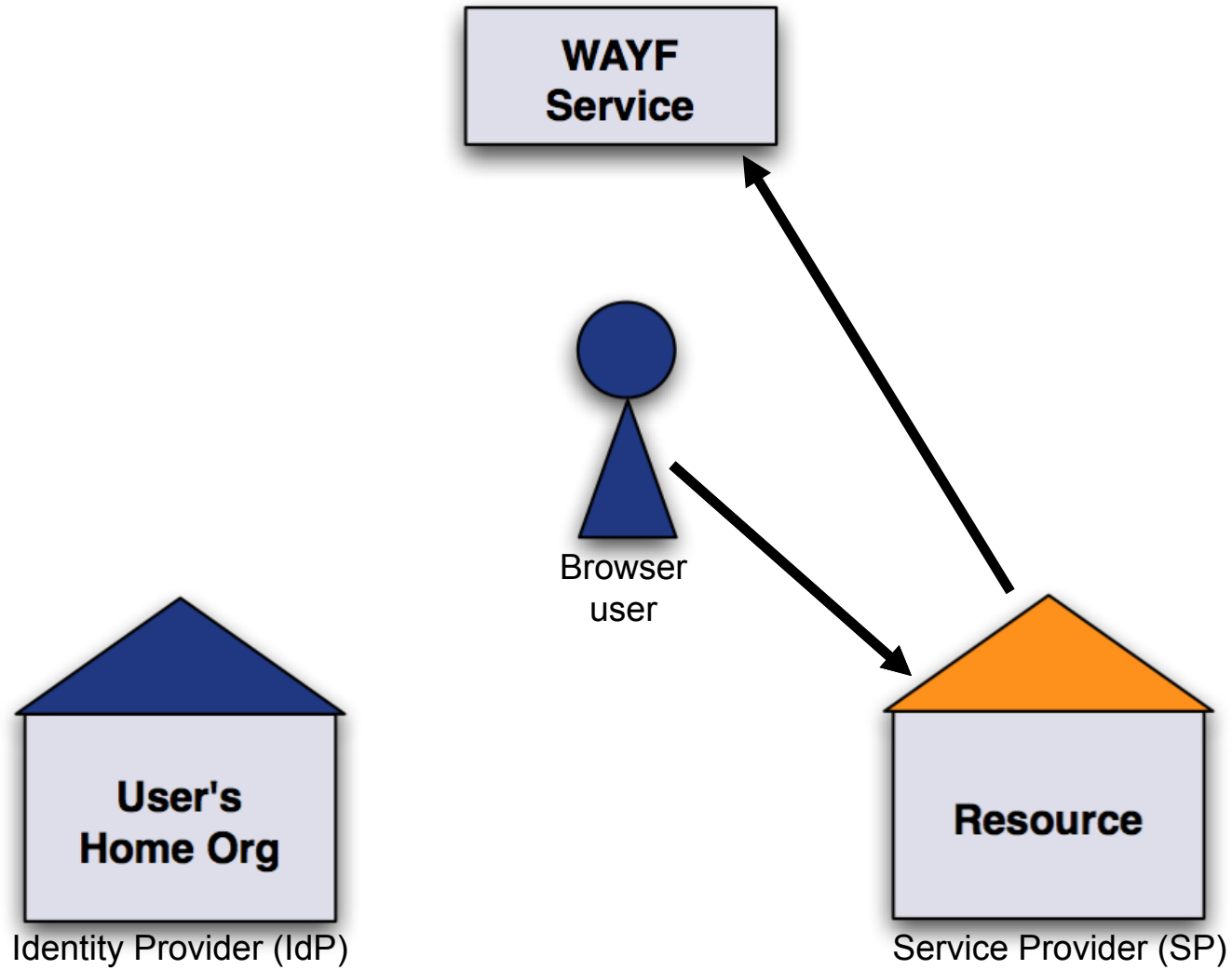
Done

start

JVCS Booking Ser... Inbox - Microsoft ... Windows Live Me... Microsoft PowerP...

11:47

# How it works





Select your home organisation

Selection options

The service you are trying to reach requires that you authenticate with your home organisation. Please select an organisation using one of the methods below.

Recent selections

- Cardiff University
- Imperial College London
- University of Edinburgh
- UKERNA Strategic Technologies

Clear

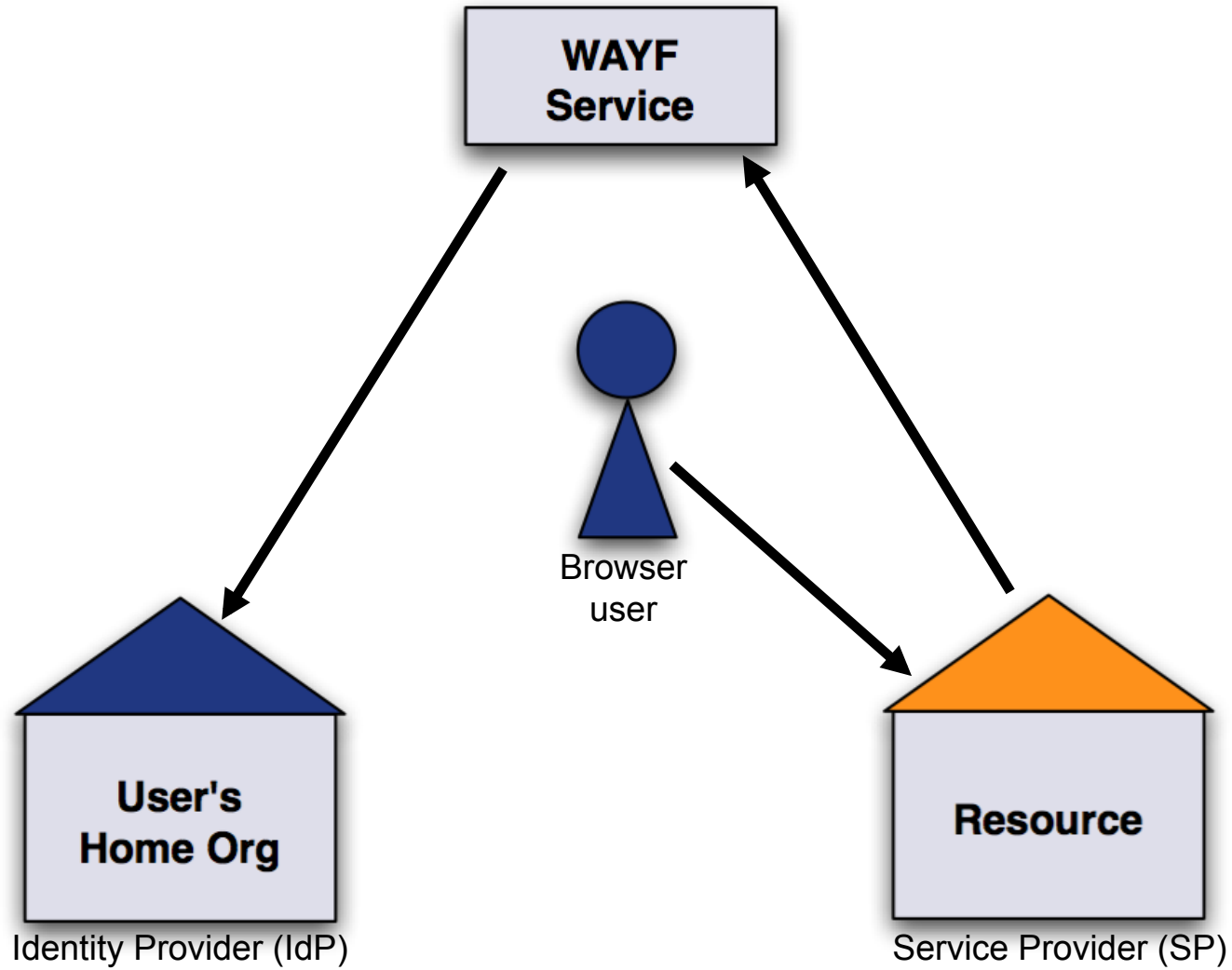
Choose from list

- AHDS, King's College
- AHDS, King's College
- AHDS, King's College (Old)
- Athens Gateway Beta
- Atomwide USO
- Birmingham Grid for Learning
- Cardiff University
- City College Plymouth
- Durham University
- Eduserv Athens
- FEAR
- i2secure
- Imperial College London
- JISC project: Angel
- JISC project: SDSS
- JISC project: SDSS (TypeKey Bridge)
- Kidderminster College
- London School of Economics and Political Science
- LSC Members Identity Service (Pilot)
- Metaleth
- MIMAS

Select

Search

# How it works





Search:  go

News & Events | Contact Us | A-Z Index



### Cardiff University Login

You have been directed here because the resource that you are attempting to view requires proof that you are a member of Cardiff University.

Enter your Cardiff University login details (**NOT your Athens account details**) to proceed:

Username:

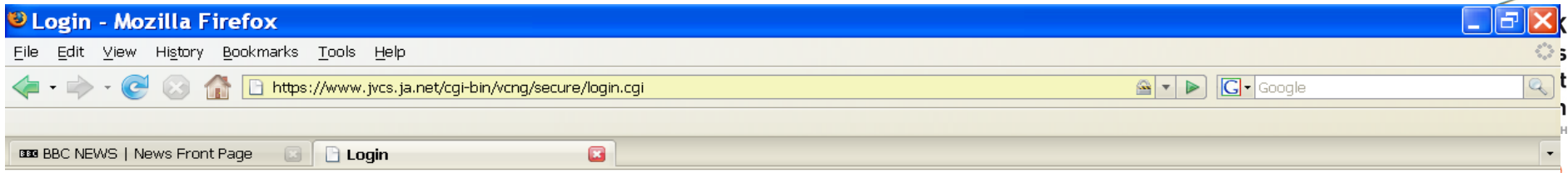


Password:

Login

You will only need to enter these details once per Web browser session. If you close your Web browser, you will be prompted to login again next time you try to access protected resources.

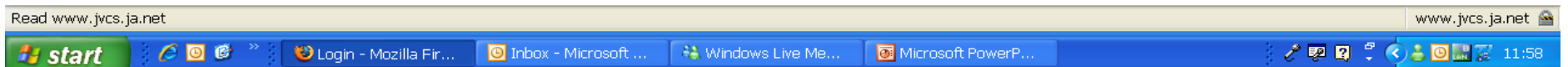
[Problems logging in?](#)



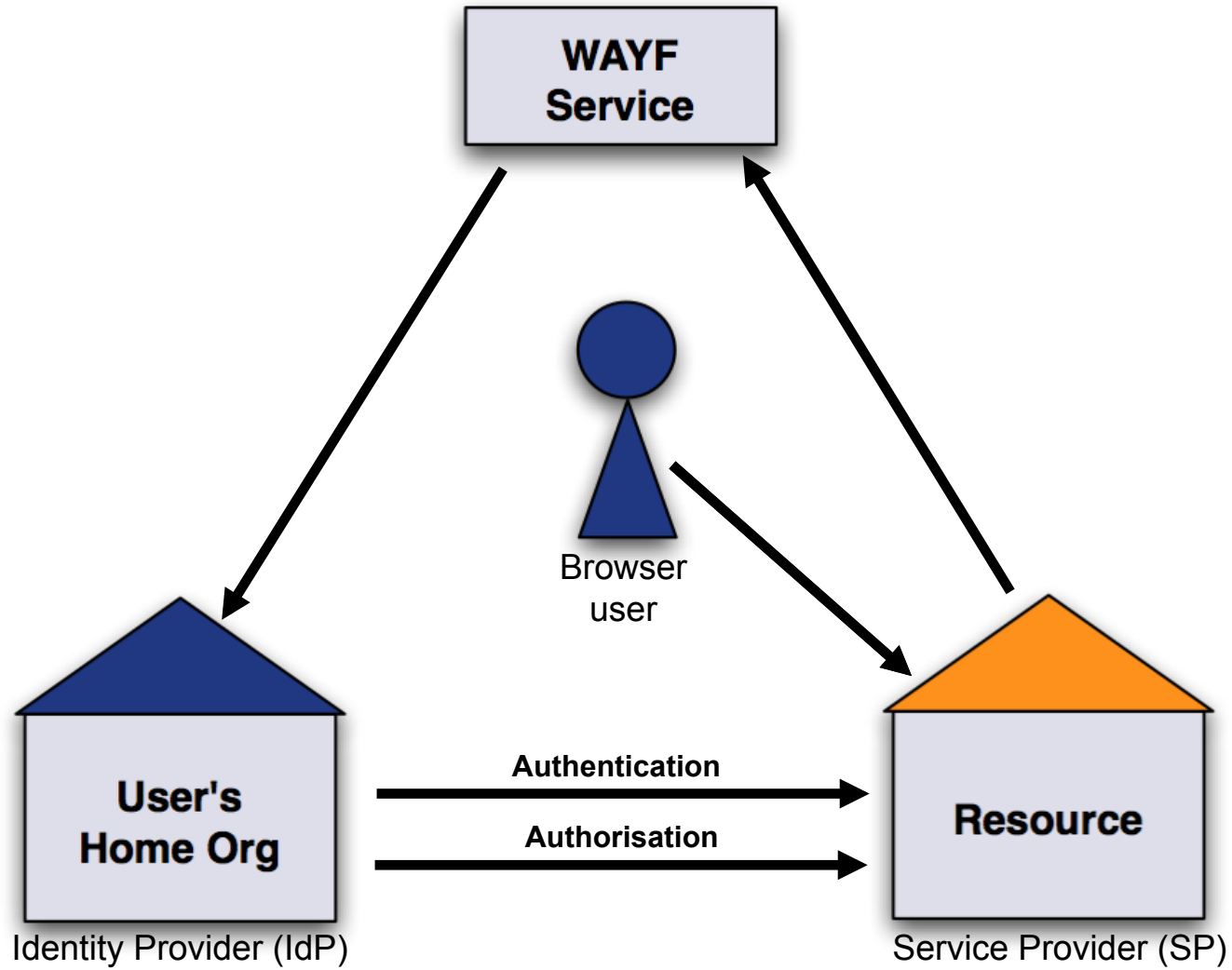
## Shibboleth Authentication Request Processed

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...



# How it works



**JVCS Booking Service home page - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

http://www.jvcs.ja.net/cgi-bin/vcng/welcome.cgi

BBC NEWS | News Front Page JVCS Booking Service home ...

**ja.net** JVCS Booking Service [Help](#) | [Logout](#) | [Home](#)

[Book videoconference](#) | [Book QA test](#) | [JVCS-Check](#) | [Book venue only](#) | [List bookings](#) | [Venue availability](#) | [Your details](#) | [Favourites list](#)  
[Administrator tasks](#)

### JVCS Booking Service home page.

**Please read the following service notes:**

- ◆ [ISDN dial-out](#) changes (05/03/07)
- ◆ [JVCS-Check](#) launched (21/11/06)
- ◆ [Venue availability](#) display in 15 minute intervals (26/09/06)

You can select a task from the menu at the top of the page or from the the list below. Alternatively, go to [JVCS-OnDemand](#).

<p><a href="#">Book videoconference</a></p> <p><a href="#">Book QA test</a></p> <p><a href="#">JVCS-Check</a></p> <p><a href="#">Book venue only</a></p> <p><a href="#">List bookings</a></p> <p><a href="#">Venue availability</a></p> <p><a href="#">Your details</a></p> <p><a href="#">Favourites list</a></p> <p><a href="#">Logout</a></p> <p>Additional tasks:</p> <p><a href="#">List organisations</a></p> <p><a href="#">List venues</a></p> <p><a href="#">List users</a></p> <p><a href="#">List groups</a></p> <p><a href="#">List regions</a></p> <p><a href="#">List sectors</a></p> <p><a href="#">Register content provider</a></p> <p><a href="#">List ISDN invoicing account owners</a></p> <p><a href="#">ISDN call charges</a></p> <hr/> <p><a href="#">Submit comment</a></p>	<p>arrange a videoconference</p> <p>arrange a Quality Assurance test for a venue</p> <p>start a JVCS-Check videoconference</p> <p>reserve a venue for a non-videoconferencing purpose</p> <p>search for and list your booked videoconferences</p> <p>show venue availability for a selected period of time</p> <p>edit your personal details and preferences</p> <p>add/edit frequently used venues and attendees</p> <p>end this session on the booking service and return to the login page</p> <p>display registered organisations</p> <p>display registered venues</p> <p>display registered users</p> <p>display organisations &amp; venues by group</p> <p>display organisations by region</p> <p>display venues by sector</p> <p>request registration of a new content provider</p> <p>display ISDN invoicing account owners</p> <p>display ISDN call charges by country</p> <hr/> <p>send a comment about the service to the development team</p>
---	---

Done

start JVCS Booking Ser... Inbox - Microsoft ... Windows Live Me... Microsoft PowerP... 12:00



# Back to... ERA plus

- ...which will enable licensed ERA Recordings to be accessed

*by students and teachers*

UK  
federation

online whether they are on the premises of their school, college or university, or at home or working elsewhere

*within the UK*

GeoLocation

# Finally

- A little more detail – how can “authorisation” work?



# Methods of “authorising”



- Simple authorisation requirements based on affiliation:
  - E.g. member/staff/student parent/governor teacher
  - Home org asserts “the user is a student”.
  - Home org knows this because their HR/SRS tells them

# Methods of “authorising”



- More complex authorisation requirements based on entitlements:
  - e.g. particular users / groups of users
  - Home org asserts “the user is part of the group allowed to access your resource”
  - Home org has to associate particular entitlements with particular users
    - Harder for home org to do, but doable for some/  
many home organisations

# Questions?



Further questions?

[www.ukfederation.org.uk](http://www.ukfederation.org.uk)

[service@ukfederation.org.uk](mailto:service@ukfederation.org.uk)