An Introduction to Federated Access Management and the UK federation

Mark Tysom, JANET(UK)

17th September 2007
Overview

• What is Authentication & Authorisation?
• What is federated access management?
• What is Shibboleth?
• What is it used for?
• How it works
• Benefits
• UK Access Management Federation
• Federations worldwide
• What’s next..?
“AA”

Authentication
• Is a user who they say they are?
  - Identity

Authorisation
• What is the user allowed to access?
  - Rights
What is federated access management?

• **Common set of rules**
  – UK federation Rules of Membership

• **Devolved authentication**
  – e.g. School, LA, RBC, College, University
Legacy access management

- User’s identity and personal data are known to all
- SP knows more than it wants and less than it needs
- Both IdP and SP need to maintain a full user database
Federated access management

- User’s identity and personal data are protected
- SP knows exactly what it needs
- SP not required to maintain a database of every user
What is Shibboleth?

• An initiative to develop an open source, standards-based solution to meet the needs for organisations to exchange information about their users in a secure, privacy-preserving manner

• Developed to meet access management needs of education
What is it used for?

• Allows a browser user to access protected online resources based on information asserted by their home organisation

• Allows providers of online resources to control access to their services
How it works
JVCS Booking Service.

The JVCS Booking Service enables registered users to create videoconferencing 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:
Forgot 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)131 660 4938 or by e-mail to vidconf@jvcs.ja.net.
How it works

Identity Provider (IdP) Service Provider (SP) Browser user

User's Home Org Resource

Copyright JNT Association 2005
Copyright JNT Association 2007
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

Choose from list

- AHDS, King's College
- AHDS, King's College
- AHDS, King's College (Old)
- Athens Gateway Beta
- Alumni Wide SO
- Birmingham Grid for Learning
- Cardiff University
- City College Plymouth
- Durham University
- Edinburgh, Athens
- EDGAR
- Dede
- Imperial College London
- JISC project Angel
- JISC project DBSS
- JISC project DBSS (Type:Key Bridge)
- Kidderminster College
- London School of Economics and Political Science
- LSC Members Identity Service (File)
- Matisse
- MIMAS

Clear

Select

Search
How it works

Browser user

User's Home Org
Identity Provider (IdP)

WAYF Service

Resource
Service Provider (SP)
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: ajones
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

WAYF Service

Browser user

User's Home Org

Identity Provider (IdP)

Authentication

Attribute Request

Authorisation

Resource

Service Provider (SP)
 JVCS Booking Service

Please read the following service notes:
- ISDN dial-out changes (provision)
- JVCS-Check launched online
- Venue availability display in 15 minute intervals (provision)

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

Book Videoconference | Book QA test | JVCS-Check | Book venue only | List bookings | Venue availability

- **Your details**
  - edit your personal details and preferences
- **Favourites list**
  - added your frequently used venues and attendees
- **Logout**
  - end this session on the booking service and return to the login page

Additional tasks:
- **List organisations**
  - display registered organisations
- **List venues**
  - display registered venues
- **List users**
  - display registered users
- **List groups**
  - display organisations & venues by group
- **List regions**
  - display organisations by region
- **List sectors**
  - display venues by sector
- **Register content provider**
  - request registration of a new content provider
- **List ISDN invoicing account owners**
  - display ISDN invoicing account owners
- **ISDN call charges**
  - display ISDN call charges by country

Submit comment
- send a comment about the service to the development team.
Attributes

• Enables fine grained AA, e.g.
  – Member of…
  – Medical student

• Not individual username and password

• SP only asks for what it needs
Benefits for Users

• Much less need to disclose your identity

• Personal data kept between you and your home organisation

• Access to online resources from anywhere

• (At least) one less password to remember
Benefits for Organisations

• Uses existing access management systems
• Can be used to protect internal resources
• Fewer support problems
• Easier to comply with regulatory requirements
  – Data Protection Act 1998
Benefits for Service Providers

• No need to maintain your own user database
  – Authentication is done for you by home organisation
  – Can authorise per institution, role, and/or entitlement

• Reduction in user support

• Reduced data protection compliance burden
  – Less storage/processing of personal data
The UK Access Management Federation for Education and Research

Mark Tysom, JANET(UK)
17th September 2007
What is the UK federation?

• A set of Rules that binds members:
  – Make accurate statements to other members
  – Keep federation systems and data secure
  – Use personal data correctly (DPA, 1998)
  – Resolve problems within the Federation
    • Not by legal action
  – Assist Federation Operator and other members
The UK federation

• Launched November 2006

• Schools, FE, HE and Research

• Organisations and institutions providing services to these sectors
Organisational Structure

• Joint funded by Becta & JISC

• Operational management by JANET(UK)

• Policy Board
  – Stakeholder representatives

• Technical Advisory Group
  – Experts from all sectors
UK federation infrastructure

– Hosted by JANET(UK)
– Discovery Service
  • Resilient WAYF
– Hosting of metadata
  • Describes the UK federation
– Monitoring of SPs and IdPs
– Test environment
– Federation web site

- [www.ukfederation.org.uk](http://www.ukfederation.org.uk)
Fully supported JANET service

- Support team at JANET(UK)
- Expert support from the JANET community
- Guidance and advice to IdPs & SPs
- Configuration guides
- Training courses
- Workshops to help organisations join the UK federation
What are the benefits?

– Provides consistency across the education sectors
– Improves the user experience
– Facilitates sharing of content and collaboration within and across sectors
– Economies of scale for both sectors
– Centrally-funded: no annual fees!
– Based on an international standard (SAML)
SAML based education federations

- Australia
- Denmark
- Finland
- France
- Norway
- Switzerland
- Sweden
- USA
What’s next…?

• UK federation development roadmap
  http://www.ukfederation.org.uk/content/Documents/DevelopmentRoadMap

  - Increase functionality
  - Enhance usability
Questions?

More info:  
www.ukfederation.org.uk

E-mail lists:  
Ukfederation-announce@jiscmail.ac.uk  
Ukfederation-discuss@jiscmail.ac.uk