An Introduction to Shibboleth and the UK Access Management Federation

Mark Tysom
Overview

• What is Authentication & Authorisation?
• What is Shibboleth?
• What is it used for?
• How it works
• Benefits
• UK Access Management Federation
• Federations worldwide
• What’s next..?
Terminology

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

Authorization (AuthZ)
• What is the user allowed to access?
  - Rights
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.
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.
AuthN & AuthZ Today

- User’s identity and personal data are known to all
- Publisher knows more than it wants and less than it needs
AuthN & AuthZ using Shibboleth

- User’s identity and personal data are protected
- Publisher knows exactly what it needs
How it works

1. Browser user
2. Service Provider (SP)
3. Identity Provider (IdP)

User's Home Org

Resource

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)
Athena Gateway Bena
Atomwide USC
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 (Type Key Bridge)
Kidderminster College
London School of Economics and Political Science
LSC Members Identity Service (Pilot)
Moodle
MIMAS

Select

Search
How it works

1. User's Home Org

2. Service Provider (SP)

3. Browser user

4. WAYF Service

5. Identity Provider (IdP)

6. Resource

Copyright JNT Association 2007
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?
How it works

1. Identity Provider (IdP)
2. Service Provider (SP)
3. Browser user
4. WAYF Service
5. User's Home Org
6. Resource
7. Authentication
8. Authorisation
9. Attribute Request
10. Authorisation
Attributes

• Allow fine grained AuthN & AuthZ.
• “Law Student” or “Staff Member” not individual username and password.
• SP can only ask for what it needs.
Benefits for Users

• Much less need to disclose your identity
• Personal data kept between you and your home organisation
• Service providers can tailor services better
• (At least) one less password to remember
• Access to online resources from anywhere
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*, etc.
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
• Users take better care of credentials
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 (inc. DPA1998)
  – Resolve problems within the Federation
    • Not by legal action
  – Assist Federation Operator and other members
The UK Federation

- Launched November 2006.
- For UK research, FE, HE and schools.
- Organisations and institutions providing services to these sectors.
Organisational Structure

- Joint funded by Becta & JISC
- Operational management by UKERNA
- Policy & Governance Board
- Technical Advisory Group
Federation infrastructure

– Discovery Service
  • Resilient WAYF
– Hosting of metadata
  • Describes the Federation
– Monitoring of SPs and IdPs
– Test environment
– Federation web site
  - www.ukfederation.org.uk
Guidance, examples, support

- How to comply with the Rules
- How to interoperate with other members
  - Common definitions, etc.
- Help in planning the transition
- Experiences of early adopters
- Reference software downloads
Support

- Guidance and advice to IdPs & SPs
- Configuration guides
- Training courses
- Workshops to help organisations join the UK Federation
- FAQs
What are the benefits?

– Provides consistency across the whole of education for AuthN & AuthZ
– Improves the user experience
– Pooling of experience and expertise
– Economies of scale for both sectors
– Facilitates sharing of content and collaboration across sectors
Global uptake

• Australia - IAM
• Denmark - DKAAl
• Finland - HAKA
• France - CRU
• Norway - FEIDE
• Switzerland - SWITCH
• USA - InCommon
What’s next…?

- “Phase Two”
- Development Roadmap
- Confederations
- Federation peering
- Convergence of local, network and application sign-in