Shibbolising UK Census and ESDS services

Lucy Bell
Associate Director, Head of Information Systems and Preservation, UKDA

26 May 2005
Today

• Our project: SAFARI
• Background: the one-stop registration service
• Introducing Shibboleth
• A model of target-to-target communication
• Comparisons
• What next?
SAFARI UKDA

- Shibboleth Authentication For Access to the Resource Infrastructures of the UKDA
- JISC-funded, 1-year project (April 2005 – March 2006)
- Aims:
  - to apply Shibboleth middleware to 3 UKDA resources
  - to embed Shibboleth technology within the one-stop registration system which is used by MIMAS, EDINA, AHDS History – all geographically dispersed
  - this should provide greater flexibility for the resource owners and, consequently, for the users
One-stop registration

• Established 2001/2002
  – Single registration for 7 resources
• Centralised registration but distributed logins
• Uses centralised Athens authentication / authorisation
• Communication occurs between resources, using strings written to users’ Athens ‘profiles’ to identify:
  – Registered users
  – Users who have agreed to certain special conditions
  – Big disadvantage: this information cannot be over-written
User is directed back to the DSU/ESDS after successful registration

User's details are stored in the UKDA database

Question: has the user registered?
Answer: yes, user logs in to use the data

Answer: no, user is taken to the registration form

Athens is updated with the information that the user has registered so they are not prompted for the form a second time

With AthensSSO the user can move between resources without logging on again
The key issue

• How to enable the dispersed resources to recognise registered users using Shibboleth (and in a way that can be over-written)?
Introducing Shibboleth

• Middleware which provides protocols for transferring user attributes from origin to target
• User authenticates locally
  – Method used is up to the origin
• User is authorised at the target
  – Method used is up to the resource, but using the attributes supplied by the origin – these attributes will be the key for us
  – Tools are available to help, such as PERMIS
Shibboleth login

Picture courtesy of SWITCH, Swiss Education & Research Network, [http://www.switch.ch/aai/demo/demo_intro.html](http://www.switch.ch/aai/demo/demo_intro.html)
Issues relating to Shibboleth

• Centralised registration = “making a cat bark”
  – Shibboleth emphasises user privacy
  – However, data owners require more controls
  – Others have approached similar resource-related identity issues

• Other advantages:
  – More fine-grained authorisation
  – Bring access control back to the resource owner
  – Complementary to Athens system, an alternative route into the data
The potential system

Shibboleth user approaches resource

User is authenticated at their originating institution

Origin provides a handle, used by Resource (DSU) to obtain user’s attributes

Resource uses attributes to determine user’s access rights AND / OR interrogates registration system

Answer: yes, user logs in to use the data

Resource uses attributes to determine user’s access rights AND / OR interrogates registration system

Question: has the user registered?

Answer: no, user is taken to the registration form

User’s details are stored in the UKDA database; registration information is a) stored somewhere and b) communicated to the DSU

User is directed back to the DSU after successful registration

These are the key parts with which SAFARI is grappling
Target-to-target communication

- Possible solutions:
  - A separate call to Essex
    - Would ensure control was within the system’s hands
    - But not necessarily standards-based
    - Doubles the risk of failure
    - Could employ session variables to allow single-sign on within one browser session
  - Establish a proxy Identity Provider (IdP)
    - Attractive alternative, but untested
    - Apply additional attributes for each resource, when logged into
    - Standards-based and recommended by Scott Cantor
    - Would still require an extra call to Essex at each authentication, which doubles the risk of failure
Comparisons already in place

- **VOSP (University of Alabama)**
  - Similar to the idea of a proxy IdP
  - \( VO = \) Service Provider within a federation
  - User is directed to their local IdP \textit{and} the VOSP to gather up all the attributes required before being authorised by the resource
  - Central attribute repository service for the VO
- **SWITCHaai, Switzerland**
  - Registration devolved to each organisation (7 signed up so far)
    - ‘Registered User’ = an attribute which origin supplies
  - Ideal but currently impractical in the UK (700+ organisations, as opposed to 7)
  - Problems of updating a registration module plug-in: special conditions would need to be stable etc.
- **Shibboleth also in production standard via HAKA Federation, Finland**
What next?

- Finalise and implement the system specification
  - Complete the establishment of the 3 targets (underway)
  - Introduce the system of target-to-target communication (Sept 05)
  - Embed within the one-stop registration system (Dec 05)
- Evaluate, via user testing/survey (Jan/Feb 06), and refine
- Write up as a case study (Feb/Mar 06)
- If model created successfully, roll out to the remaining services (post Mar 06)
More information

- Project Manager: Lucy Bell (lajbell@essex.ac.uk)

- Project web site: http://safari.data-archive.ac.uk (available June 05)