

# Deploying web user authentication with Shibboleth

Sören Preibusch

Then said they unto him, Say now Shibboleth:  
and he said Shibboleth



Shibboleth

raven: Elise Øygaard

# Agenda

**1**

**what, why, when: Shibboleth basics**

**2**

**how: Interaction scenarios**

**3**

**who: privacy issues**

**4**

**whoops: pitfalls and hints**

# What is Shibboleth?

- The Shibboleth System is a
  - ▬ standards based,
  - ▬ open source software package
  - ▬ for web single sign-on
  - ▬ across or within organizational boundaries.
- It allows sites to make
  - ▬ informed authorization decisions
  - ▬ for individual access of protected online resources
  - ▬ in a privacy-preserving manner.



**Shibboleth**<sup>®</sup>

<http://shibboleth.internet2.edu/about.html>

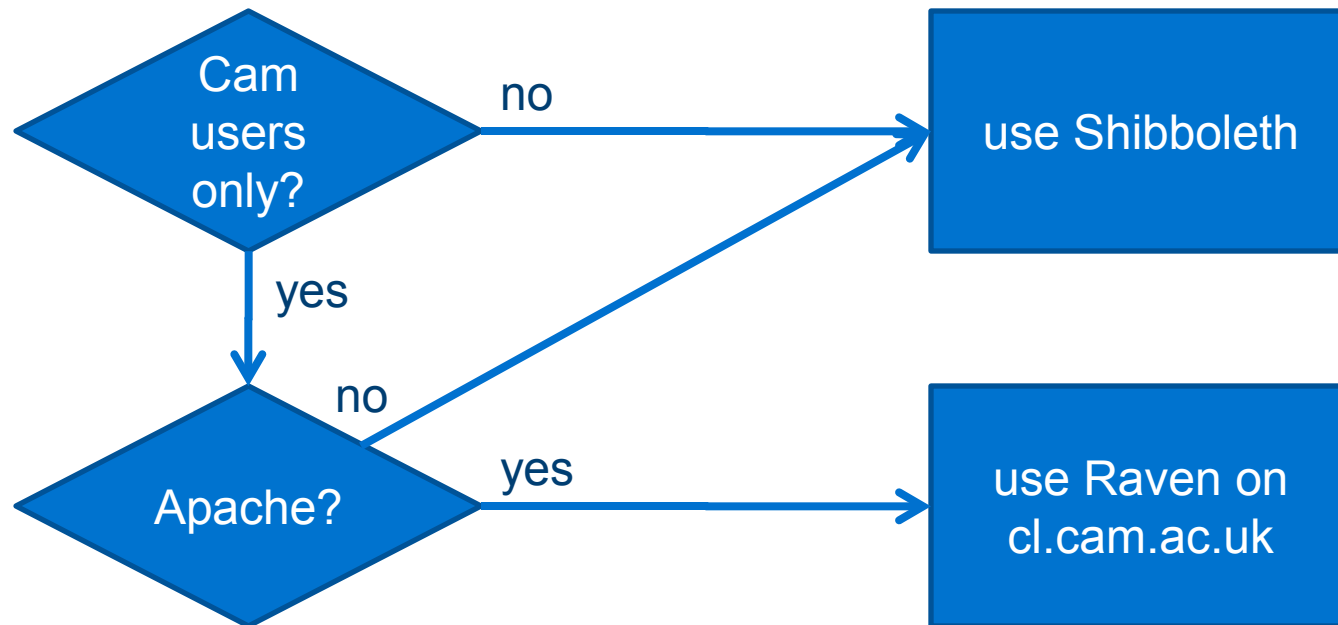
# Shibboleth in practice

- Authentication and authorisation system for Web resources
- Similar to Raven, but
  - ▬ standardised
  - ▬ globally cross-organisational
  - ▬ successor to Athens (funding stopped June 2008)
  - ▬ perceivedly slower
- cf. eduroam



# Why and when

- authenticate people – not IP addresses
- do not proliferate authentication systems



# Agenda

1

**what, why, when: Shibboleth basics**

2

**how: Interaction scenarios**

3

**who: privacy issues**

4

**whoops: pitfalls and hints**

# Example: Shibboleth authentication (1)

The screenshot displays the EDINA website interface. At the top, there is a navigation bar with links for Help & Support, About, Feedback, Contact, Site Map, and a search box. Below this is the EDINA logo and the tagline "providing resources for staff and students in higher and further education in the UK and beyond". A secondary navigation bar contains dropdown menus for "Services" and "Projects", each followed by a "Go" button.

The main content area is organized into three columns of service categories:

- Reading & Reference:** Includes Article References, CAB Abstracts, Land Life Leisure, Journal Catalogues, SUNCAT (UK), SALSER (Scottish), E-books (The Statistical Accounts of Scotland), Deposit Academic Papers, and the Depot.
- Maps & Data:** Includes Geo-data Portal, Go-Geol, Maps & Datasets, Digimap - Ordnance Survey, Geology Digimap, Historic Digimap, Marine Digimap, UKBORDERS, Agricultural Census Data, agcensus, Deposit Data, and ShareGeo facility.
- Multimedia & Education:** Includes Film, Images & Sound, Education Image Gallery, Film & Sound Online, NewsFilm Online, Learning Materials, Jorum User, Deposit Learning Materials, and Jorum Contributor.

On the right side, there is a "News, Training & Events" section with several news items and a "Quarterly Newsletter" link. Below this are three boxes: "Ways to contribute online", "Our projects and middleware", and "For library and support staff".

At the bottom left, there is a legend: "📄 = open to all" and a link "What services can I use?". The footer contains the text: "EDINA is a JISC National Data Centre based at the University of Edinburgh | Accessibility | Acknowledgements". The JISC logo is positioned in the bottom right corner of the page.



# Example: Shibboleth authentication (2)

The screenshot shows the EDINA Digimap Collections website. At the top, there is a navigation bar with links for Help & Support, About, Feedback, Contact, Site Map, and a search box. The main header is blue with the text "Digimap Collections". Below this, a breadcrumb trail reads "You are here: EDINA > Digimap Collections".

The main content area is titled "Login to Digimap Collections" and includes the following text: "Online maps and spatial data of Great Britain for UK HE and FE." Below this is a "Login" button with a right-pointing arrow, followed by the text "via UK federation. [info]". There are also links for "To which Digimap Collections does your institution subscribe?" and "Having trouble logging in?".

A notice states: "Digimap will be making use of the 'at risk' period between 17.30 and 20.00 hours on Tuesday 26th May. All Digimap collections will be unavailable between these times. We apologise for any inconvenience caused."

Logos for partner organizations are displayed: Ordnance Survey, LANDMARK Information Group, OGC (Open Geospatial Consortium, Inc.), SeaZone, and British Geological Survey (NATURAL ENVIRONMENT RESEARCH COUNCIL).

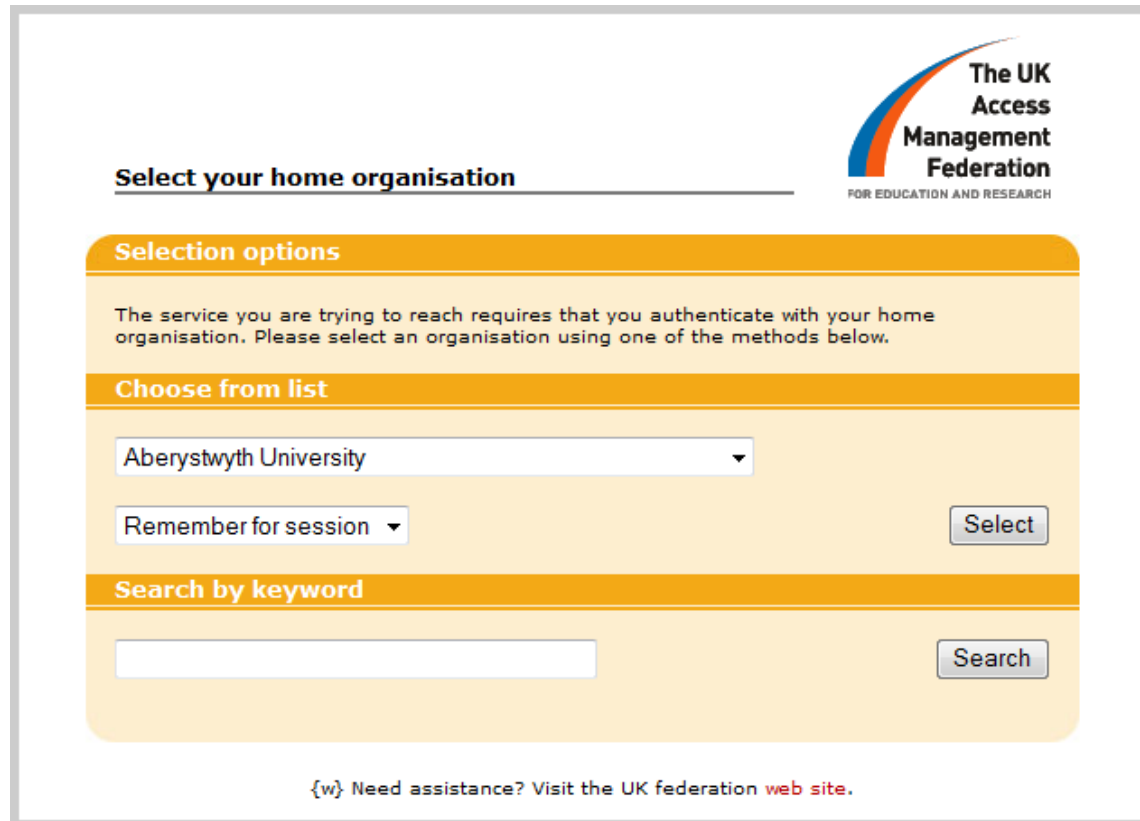
On the left, a "Digimap Collections Menu" is visible with items: Login, Description, Access & Subscription, Help & Support, and EDINA News & Events. Below the menu is the text "For Library & Support Staff".

On the right, a "Related Links" section contains: Maps & Data, agcensus, UKBORDERS, Go-Geo!, and Digimap Blog. Below that is a "Digimap News" section with the heading "Check out ShareGeo!" and text: "ShareGeo is a new geospatial data sharing facility. Find, contribute and share geospatial data with other Digimap users. Access is from the Digimap Collections page after logging in. More information about ShareGeo."

At the bottom, it says "EDINA is a JISC National Data Centre based at the University of Edinburgh | Accessibility | Acknowledgements" and features the JISC logo.

invitation to login

# Example: Shibboleth authentication (3)



The screenshot shows the login interface for the UK Access Management Federation. At the top right is the logo for 'The UK Access Management Federation FOR EDUCATION AND RESEARCH'. Below the logo, the text 'Select your home organisation' is followed by a horizontal line. The main content area is divided into three sections: 'Selection options', 'Choose from list', and 'Search by keyword'. The 'Selection options' section contains a paragraph explaining the authentication requirement. The 'Choose from list' section features a dropdown menu with 'Aberystwyth University' selected, a 'Remember for session' dropdown, and a 'Select' button. The 'Search by keyword' section has a text input field and a 'Search' button. At the bottom, there is a link for assistance: '{w} Need assistance? Visit the UK federation web site.'

**The UK Access Management Federation**  
FOR EDUCATION AND RESEARCH

**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.

**Choose from list**

Aberystwyth University ▼

Remember for session ▼


**Search by keyword**

{w} Need assistance? Visit the UK federation [web site](#).

[https://wayf.ukfederation.org.uk/shibboleth-wayf/...](https://wayf.ukfederation.org.uk/shibboleth-wayf/)


# Example: Shibboleth authentication (4)

[help](#)

 UNIVERSITY OF  
CAMBRIDGE

## Raven Authentication Service

University of Cambridge > Computing Service > Raven



**RAVEN**

The web resource you requested requires you to identify yourself [[help - why am I seeing this?](#)]. This resource calls itself '**the Raven/Shibboleth authentication server**' and is provided by the website `shib.raven.cam.ac.uk`. You should only proceed if you are happy to be identified to this site.

User-id:

Password:

override login options for this session?

[\[help\]](#)

**Always** quit your web browser when you have finished accessing services that require authentication. Do not disclose your Raven password to anyone and only enter it on web pages with URLs that start `https://raven.cam.ac.uk/`. Please report attempts to obtain your password by other means.


**UCS**

The Raven web authentication system is provided and managed by the [University Computing Service](#).  
© 2009 University of Cambridge Computing Service

<https://raven.cam.ac.uk/auth/authenticate.html?...>


# Example: Shibboleth authentication (5)

[help](#)

 UNIVERSITY OF CAMBRIDGE

**Raven Authentication Service**

University of Cambridge > Computing Service > Raven



### Information Release

I agree to the following information being disclosed to 'EDINA: Digimap (live)' both now and when I access this site in the future.

**eduPerson Principal Name:** sdp36@cam.ac.uk

**Anonymous identifier:** Lmju6PfXZg1TM2zeOBEURCv2rtI=@cam.ac.uk

**Status:** member@cam.ac.uk  
member@eresources.lib.cam.ac.uk

**Entitlement:** urn:mace:dir:entitlement:common-lib-terms

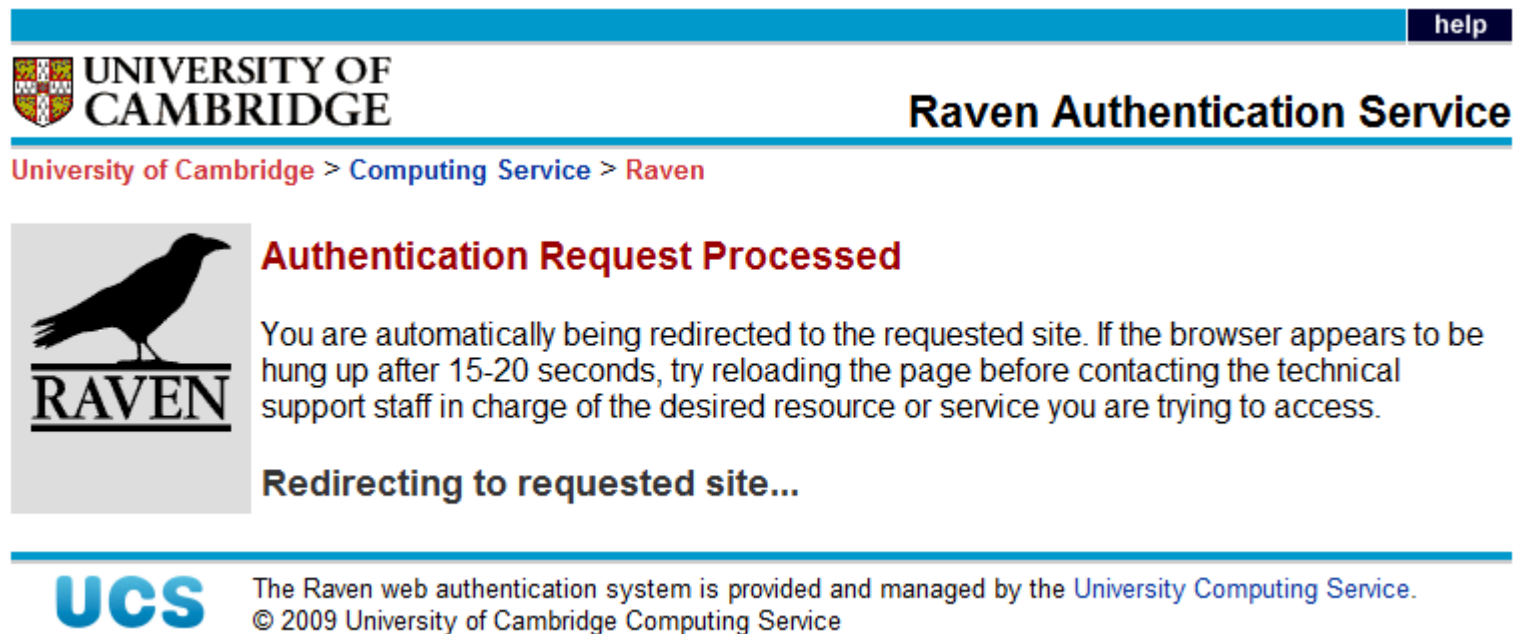
[\[help\]](#)

---

**UCS** The Raven web authentication system is provided and managed by the [University Computing Service](#).  
© 2009 University of Cambridge Computing Service


<https://shib.raven.cam.ac.uk/arpviewer/...>

# Example: Shibboleth authentication (6)




The screenshot shows the Raven Authentication Service interface. At the top right is a 'help' button. The University of Cambridge logo and name are on the left, and the title 'Raven Authentication Service' is on the right. A breadcrumb trail reads 'University of Cambridge > Computing Service > Raven'. Below this is a large grey box containing a black silhouette of a raven perched on a branch above the word 'RAVEN'. To the right of this box is the heading 'Authentication Request Processed' in red, followed by a paragraph of text explaining the redirection process. Below the text is the phrase 'Redirecting to requested site...'. At the bottom left is the 'UCS' logo, and to its right is a footer paragraph stating that the system is provided and managed by the University Computing Service, with a copyright notice for 2009.

help

 UNIVERSITY OF CAMBRIDGE

Raven Authentication Service

University of Cambridge > Computing Service > Raven

 **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...**

**UCS** The Raven web authentication system is provided and managed by the [University Computing Service](#).  
© 2009 University of Cambridge Computing Service

<https://shib.raven.cam.ac.uk/shibboleth-idp/...>

# Example: Shibboleth authentication (7)

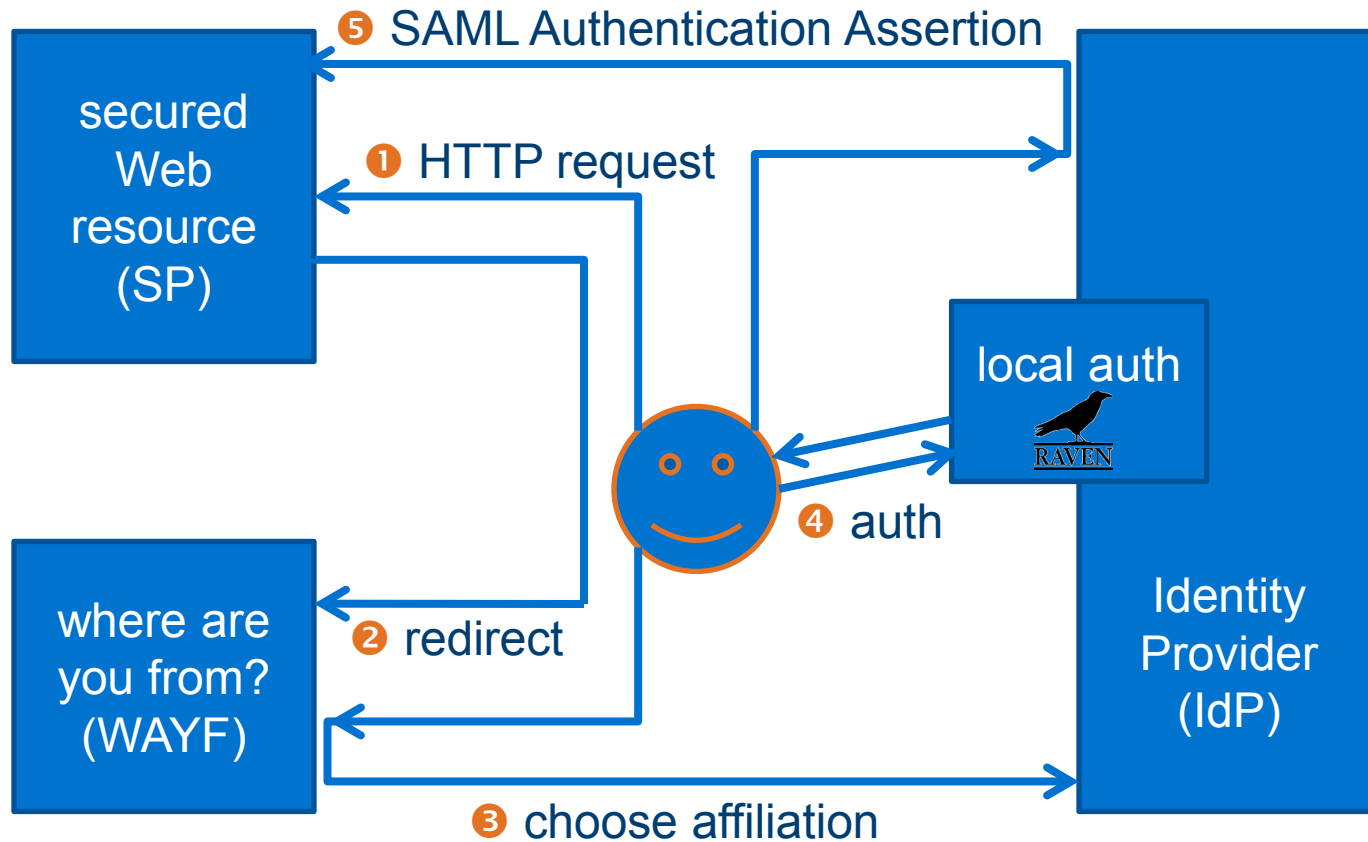
The screenshot shows the Digimap website interface. At the top left is the Digimap logo, and at the top right is the EDINA logo with a "Log-Out" link. The main content is organized into several sections:

- TODAY'S MESSAGES:**
  - Licence Numbers:** A message explaining that users are asked for a "Digimap Licence Number" and should use their institution's OS Educational Copyright Licence number. A link to a blog post for more explanation is provided.
  - Digimap Blog** and **Digimap News** links are shown with small icons.
  - Check out ShareGeo!** A message stating that ShareGeo is a new geospatial data repository where users can add their own spatial datasets for sharing.
- Map and Data Collections:**
  - Ordnance Survey Collection †**: Contemporary Ordnance Survey maps and map data. Includes a "More information" link.
  - Historic Digimap †**: Historical Ordnance Survey maps from 1843 to 1996. Includes a "More information" link.
  - Geology Digimap †**: Current British Geological Survey map data and Lexicon of named Rock Units. Includes a "More information" link.
  - Marine Digimap †**: Hydrographic and marine data from SeaZone Solutions Ltd. Includes a "More information" link.
- Find and Share:**
  - Go-Geo! †**: Search for geospatial data, information and services. Includes a "More information" link.
  - ShareGeo (Beta) ‡**: Find, contribute and share geospatial data with others. Includes a "More information" link.
  - GeoDoc †**: Create geospatial metadata for publication in Go-Geo!.
- Tools/Developer's Area:**
  - A message stating: "This is a new area which will be available in the near future. In the meantime, find out about the GeoCrossWalk gazetteer and Digimap mapping APIs in the Ordnance Survey Collection. Separate registration will be required in order to use these."

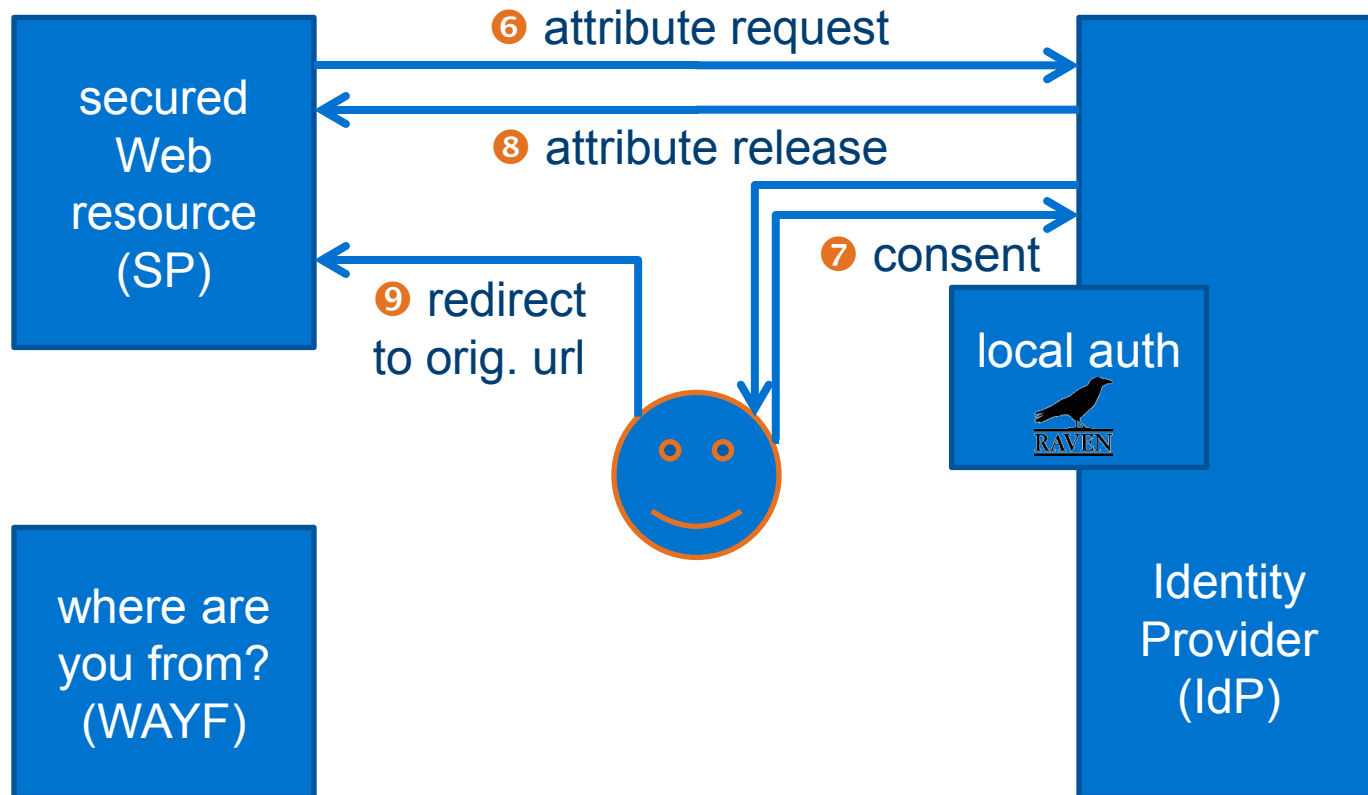
At the bottom, there is a JISC logo with the text "JISC † JISC funded ‡ JISC supported". The footer of the page reads "© University of Edinburgh."

<http://digimap.edina.ac.uk/>

# Shibboleth interaction revisited: authentication



# Shibboleth interaction revisited: authorisation



Jon Warbrick



# Scaling up

- **rôle-based** authorisation (e.g. member@cam.ac.uk)
- **federations** for institutional trust (e.g. UK Federation)
  
- IdPs and SPs agree on
  - ▬ trust (authentication)
  - ▬ attribute semantics (authorisation)

# Agenda

1

**what, why, when: Shibboleth basics**

2

**how: Interaction scenarios**

3

**who: privacy issues**

4

**whoops: pitfalls and hints**

# Attribute release

- SPs may communicate needed attributes
- attribute release governed by IdP
- IdP may favour some federations (e.g. Raven / Ucam Federation)
- user has **take-it-or-leave-it** choice
  
- pseudonyms (RBAC) and identities (only one at a time)

# UK federation core attributes

I agree to the following information being disclosed to 'EDINA: D...  
and when I access this site in the future

<b>eduPerson Principal Name:</b>	sdp36@cam.ac.uk
<b>Anonymous identifier:</b>	Lmju6PfXZg1TM2zeOBEURCv2rtI=@cam.ac.uk
<b>Status:</b>	member@cam.ac.uk member@eresources.lib.cam.ac.uk
<b>Entitlement:</b>	urn:mace:dir:entitlement:common-lib-terms

[\[help\]](#)

The diagram shows two blue boxes with white text. The first box, labeled 'EPPN', has a blue arrow pointing to the 'eduPerson Principal Name' field. The second box, labeled 'eduPersonTargetedId', has a blue arrow pointing to the 'Anonymous identifier' field.

# Ucam federation attribute release

Shib-Application-ID: default  
Shib-Session-ID: \_c0582d05b229d54d085a14fb74ee1003  
Shib-Identity-Provider: https://shib.raven.cam.ac.uk/shibboleth  
Shib-Authentication-Instant: 2009-05-18T11:36:59.165Z  
Shib-Authentication-Method: urn:oasis:names:tc:SAML:1.0:am:unspecified  
Shib-AuthnContext-Class: urn:oasis:names:tc:SAML:1.0:am:unspecified  
affiliation: member@cam.ac.uk;member@eresources.lib.cam.ac.uk  
cn: S.D. Preibusch  
displayName: Sören Preibusch  
entitlement: urn:mace:dir:entitlement:common-lib-terms  
epn: sdp36@cam.ac.uk  
instID: CL  
jdInst: CL  
mail: sdp36@cam.ac.uk  
mailAlternative: Soren.Preibusch@cl.cam.ac.uk  
misAffiliation: student  
ou: Computer Laboratory  
persistent-id: https://shib.raven.cam.ac.uk/shibboleth!https://elbe.ad.cl.cam.ac.uk/local-only!/K48zwTsLnLfwAKBerFuV597VKs=  
sn: Preibusch  
targeted-id: /K48zwTsLnLfwAKBerFuV597VKs=@cam.ac.uk  
telephoneNumber: 63668 (Computer Laboratory office)  
remote-user: sdp36@cam.ac.uk

lookup.cam.ac.uk

# Agenda

1

**what, why, when: Shibboleth basics**

2

**how: Interaction scenarios**

3

**who: privacy issues**

4

**whoops: pitfalls and hints**

# the Cake Survey

## Cake Feedback

Dear DTG member,

Please help us to improve our Monday cake supply for the upcoming term by completing the short questionnaire below.

In kind appreciation of your cooperation,  
Sören & Usman

1. I am a regular participant of the DTG Monday meeting.

- yes  
 no

... and of the Monday cake session.

- yes  
 no

2. My preferred cake variety so far has been:

- chocolate cake  
 double-chocolate cake  
 triple-chocolate cake  
 double-chocolate gateau  
 cheese cake  
 profiterole gateau  
 lemon cake  
 lemon-cheese cake  
 Madeira party cake

3. Please indicate your satisfaction with the following supermarkets and bakeries from which we have sourced in the past:

- Asda
- Fitzbillies
- Sainsbury's
- Tesco

We are also considering alternative suppliers:

- Aldi
- Waitrose

4.  I would like to see more regional specialities.

5.  I suffer from allergies and incompatibilities.

6.  I have dietary requirements.

7.  I am a responsible consumer.

# Shibboleth installation on IIS 7

- installing Raven on **IIS 7** will mess up the system
  - some non-default IIS modules needed
  - Shibboleth comes as binary installer, restart required
  - integrates as ISAPI module
  - SSL support optional
  - no interference with existing auth mechanisms
- ⇒ roughly hassle-free



# Configuring Shibboleth

- XML configuration files, pre-configured by UCS
- Server details: `<Site id="1" name="elbe.ad.cl.cam.ac.uk"/>`
- Redirects: `<ApplicationDefaults id="default" policyId="default" entityID="https://elbe.ad.cl.cam.ac.uk/local-only/" homeURL="https://elbe.ad.cl.cam.ac.uk/local-only/" REMOTE_USER="eppn persistent-id targeted-id" signing="false" encryption="false">`
- SSL: `<Sessions handlerSSL="true"`
- miscellaneous metadata (contact information, ...)

# Defining access control rules

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="elbe.ad.cl.cam.ac.uk">
      <Path name="local-only" authType="shibboleth" requireSession="true">
        <AccessControl>
          <!-- <Rule require="groupID">101065</Rule> -->
          <!-- <Rule require="instID">CL</Rule> -->
          <RuleRegex require="user">@cam.ac.uk$</RuleRegex>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
```

# Expressive language for access control rules

- individual enumerable users  
`<Rule require="user">arb33@cam.ac.uk acr31@cam.ac.uk</Rule>`
- explicit rule disjunction  
`<OR> <Rule ... /> <Rule ... /> </OR>`
- regular expressions:  
`<RuleRegex require="user">@cam.ac.uk$</RuleRegex>`
- lookup.cam group membership  
`<Rule require="groupID">100852</Rule>`
- lookup.cam institution membership  
`<Rule require="instID">CS</Rule>`
- authentication only / optionally

Debugging is hard!

# Joining the Ucam Federation

- Federation stores metadata about SP
- IdP displays SP-specific metadata during authentication
  - ≡ “I agree to the following information being disclosed to 'unknown Service Provider' ...”
- Advantages:
  - ≡ named SP
  - ≡ more attributes
  - ≡ hassle-free

# Additional resources

- <https://wiki.csx.cam.ac.uk/raven/Raven/Shibboleth>
- [raven-support@ucs.cam.ac.uk](mailto:raven-support@ucs.cam.ac.uk)
- "cs-raven-discuss" mailing list
- <http://shibboleth.internet2.edu>

# Thank you very much.

**Questions and comments**

are welcome and highly appreciated.

[sdp36@cam.ac.uk](mailto:sdp36@cam.ac.uk)