UNIVERSITY OF CAMBRIDGE
800 YEARS
1209 ~ 2009

Deploying web user authentication with Shibboleth

Sören Preibusch

Computer Laboratory

18th May 2009

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

Shibboleth

raven: Elise Øygard

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.

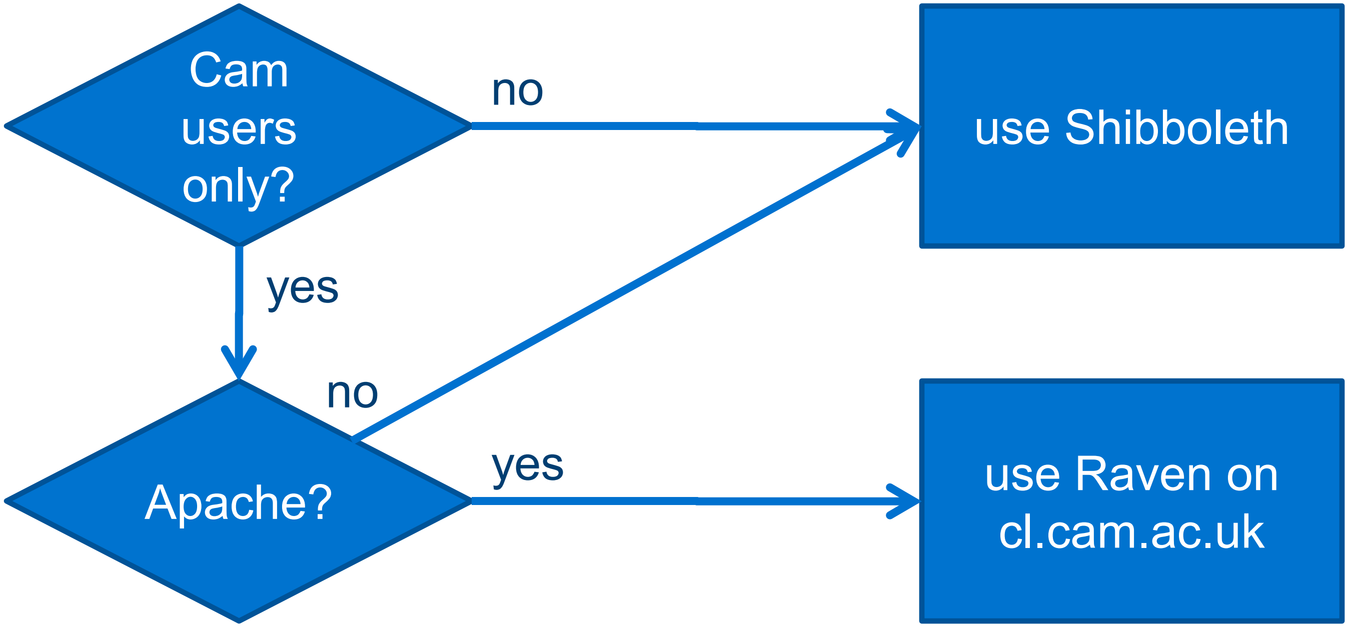
http://shibboleth.internet2.edu/about.html

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

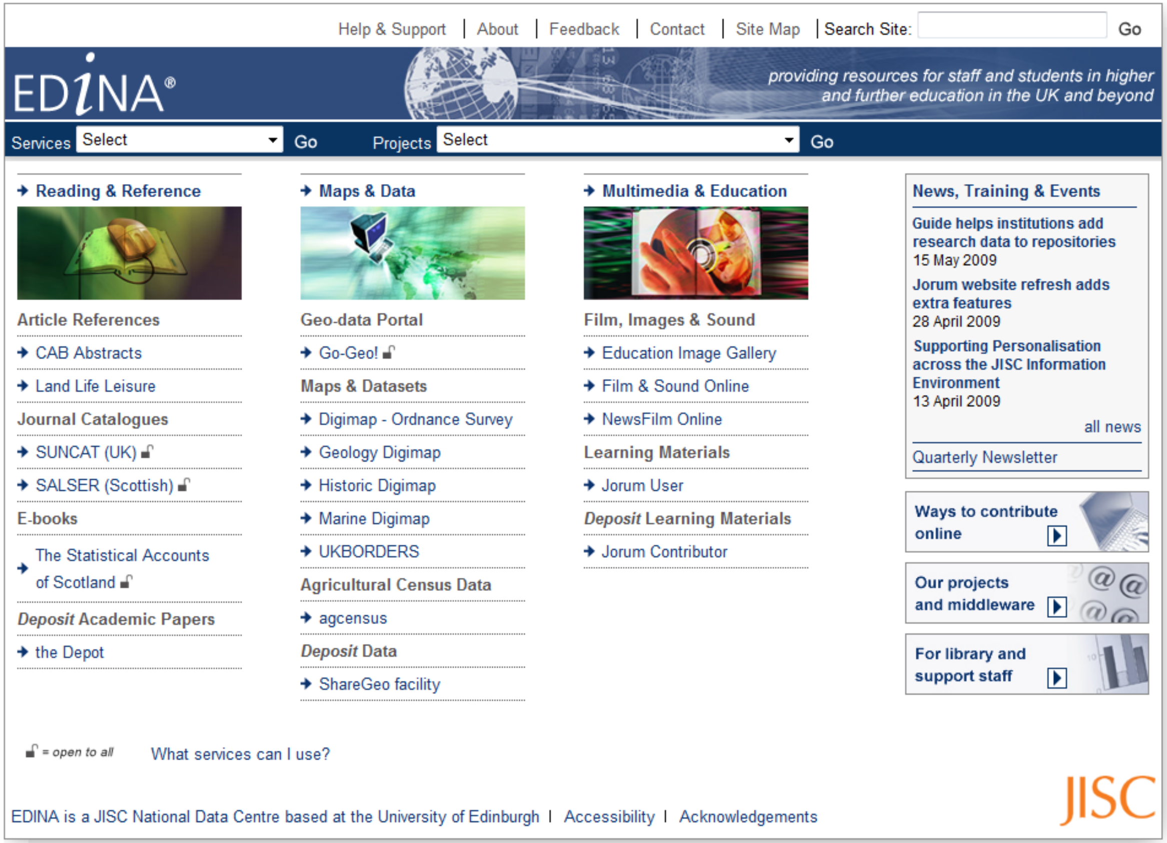
1 what, why, when: Shibboleth basics

2 how: Interaction scenarios

3 who: privacy issues

4 whoops: pitfalls and hints

Example: Shibboleth authentication (1)



Help & Support | About | Feedback | Contact | Site Map | Search Site: Go

EDINA®

providing resources for staff and students in higher and further education in the UK and beyond

Services Select Go Projects Select Go

Reading & Reference

Article References
- CAB Abstracts
- Land Life Leisure

Journal Catalogues
- SUNCAT (UK) 🔓
- SALSER (Scottish) 🔓

E-books
- The Statistical Accounts of Scotland 🔓

Deposit Academic Papers
- the Depot

Maps & Data

Geo-data Portal
- Go-Geo! 🔓

Maps & Datasets
- Digimap - Ordnance Survey
- Geology Digimap
- Historic Digimap
- Marine Digimap
- UKBORDERS

Agricultural Census Data
- agcensus

Deposit Data
- ShareGeo facility

Multimedia & Education

Film, Images & Sound
- Education Image Gallery
- Film & Sound Online
- NewsFilm Online

Learning Materials
- Jorum User

Deposit Learning Materials
- Jorum Contributor

News, Training & Events

Guide helps institutions add research data to repositories
15 May 2009

Jorum website refresh adds extra features
28 April 2009

Supporting Personalisation across the JISC Information Environment
13 April 2009

all news

Quarterly Newsletter

Ways to contribute online

Our projects and middleware

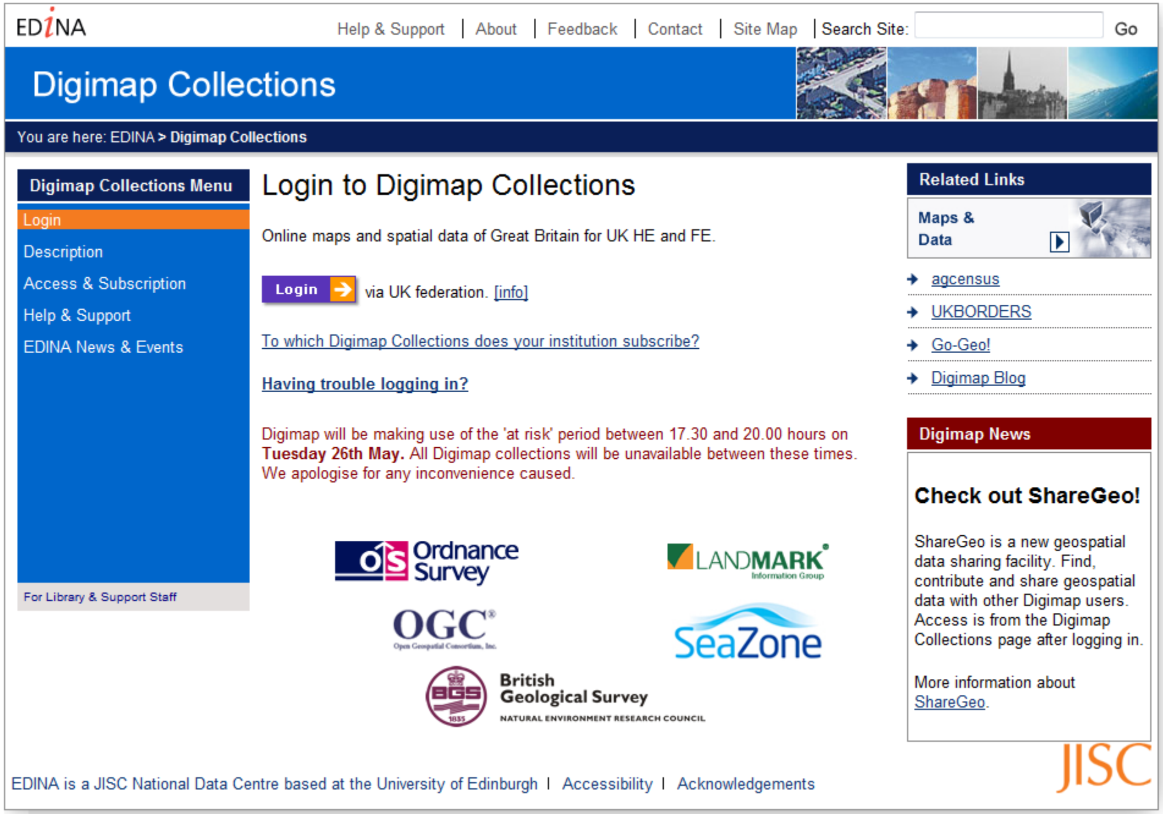
For library and support staff

🔓 = *open to all* What services can I use?

EDINA is a JISC National Data Centre based at the University of Edinburgh | Accessibility | Acknowledgements

JISC

Example: Shibboleth authentication (2)



EDiNA
Help & Support | About | Feedback | Contact | Site Map | Search Site: Go

Digimap Collections

You are here: EDINA > **Digimap Collections**

Login to Digimap Collections

Online maps and spatial data of Great Britain for UK HE and FE.

via UK federation. [info]

To which Digimap Collections does your institution subscribe?

Having trouble logging in?

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.

Ordnance Survey
LANDMARK Information Group
OGC Open Geospatial Consortium, Inc.
SeaZone
BGS
British Geological Survey
NATURAL ENVIRONMENT RESEARCH COUNCIL

Check out ShareGeo!

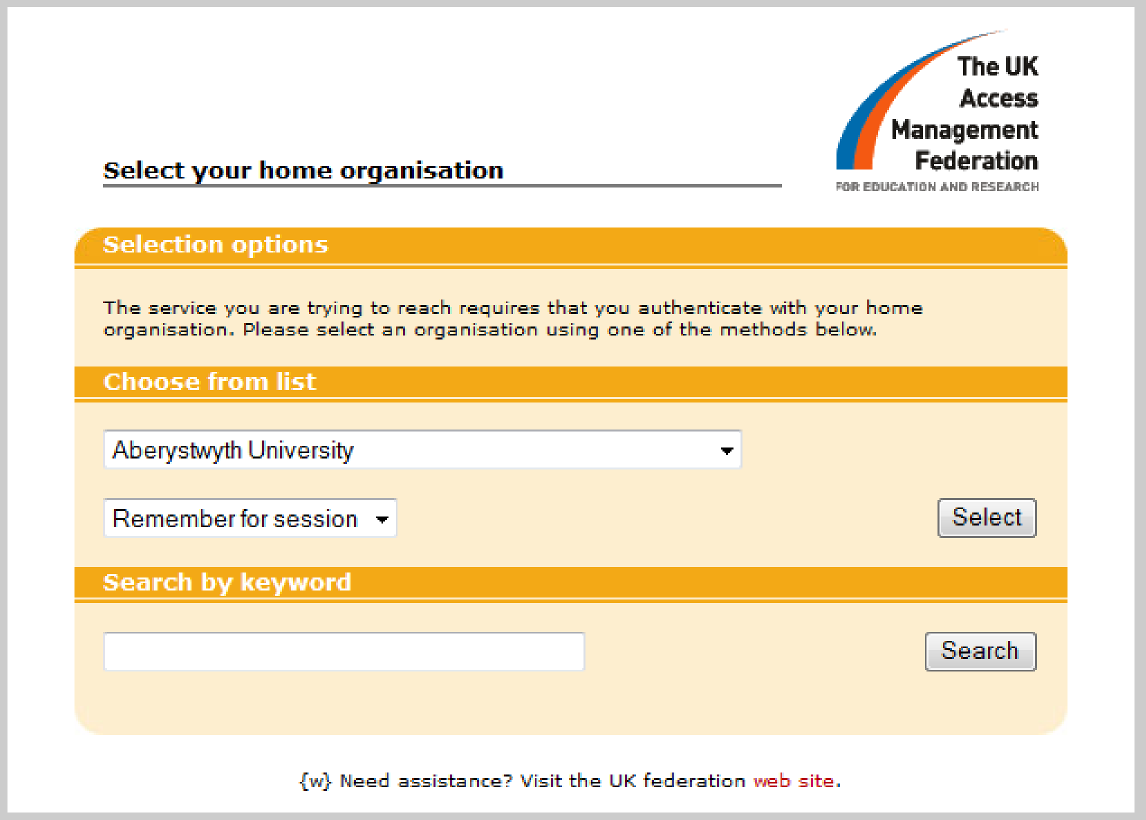
ShareGeo is a new geospatial data sharing facility. Find, contribute and share geospatial data with other Digimap users. Access is from the Digimap Collections page after logging in.

More information about ShareGeo.

EDINA is a JISC National Data Centre based at the University of Edinburgh | Accessibility | Acknowledgements

invitation to login

Example: Shibboleth authentication (3)



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

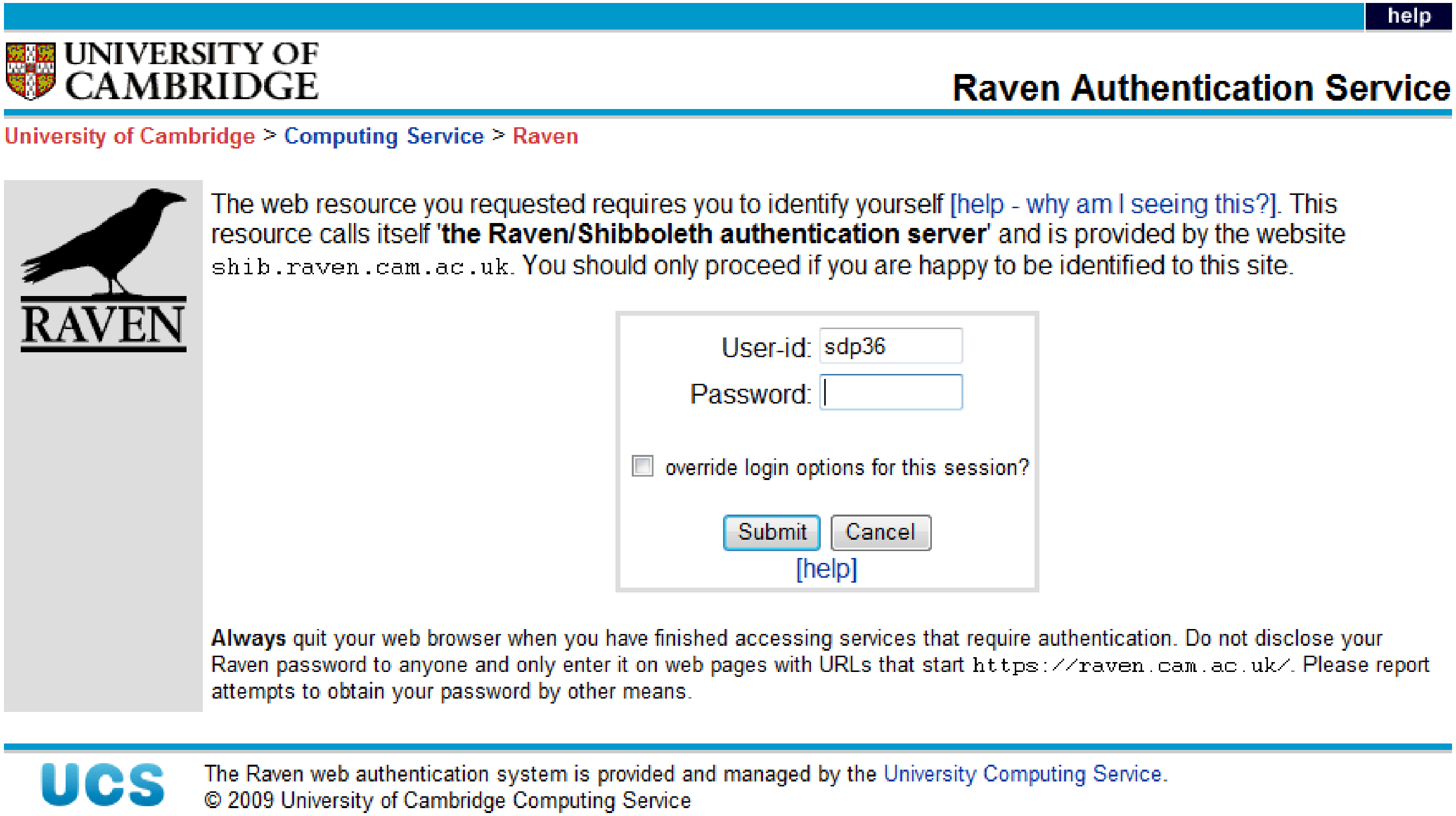
Remember for session

Search by keyword

{w} Need assistance? Visit the UK federation web site.

https://wayf.ukfederation.org.uk/shibboleth-wayf/...

Example: Shibboleth authentication (4)



UNIVERSITY OF CAMBRIDGE

Raven Authentication Service

University of Cambridge > Computing Service > 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: sdp36

Password:

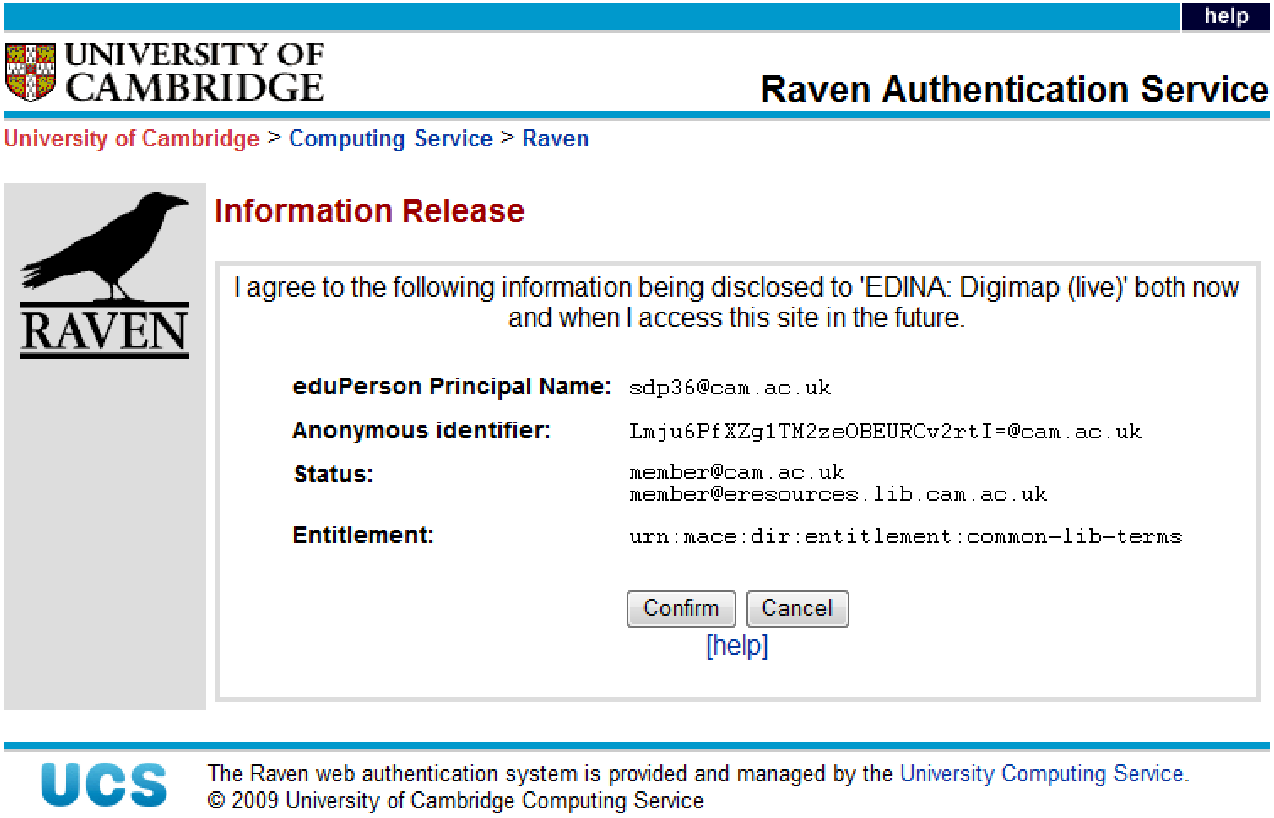
□ override login options for this session?

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.

The Raven web authentication system is provided and managed by the University Computing Service.

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

Example: Shibboleth authentication (5)



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`

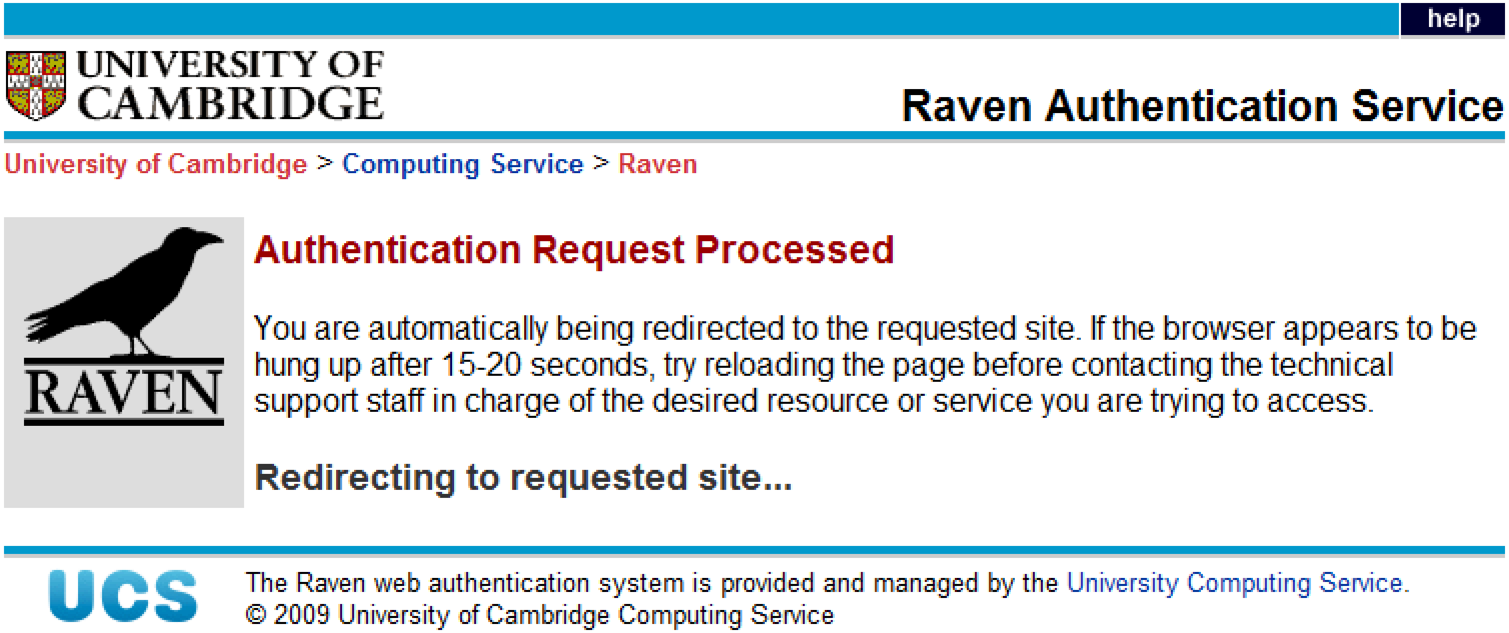
Confirm Cancel

[help]

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)



Raven Authentication Service

University of Cambridge > Computing Service > Raven

Authentication Request Processed

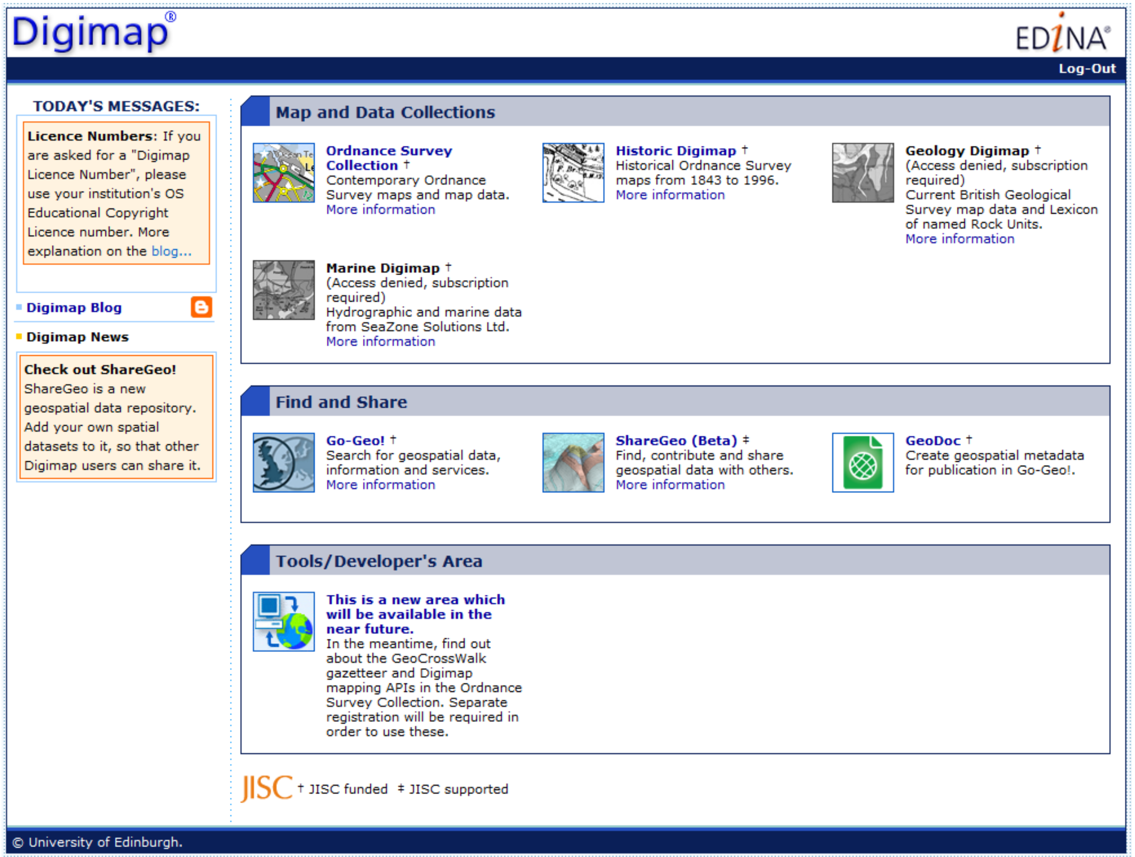
You are automatically being redirected to the requested site. If the browser appears to be hung up after 15-20 seconds, try reloading the page before contacting the technical support staff in charge of the desired resource or service you are trying to access.

Redirecting to requested site...

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)



Digimap®

EDINA®

TODAY'S MESSAGES:

Licence Numbers: If you are asked for a "Digimap Licence Number", please use your institution's OS Educational Copyright Licence number. More explanation on the blog...

Check out ShareGeo! ShareGeo is a new geospatial data repository. Add your own spatial datasets to it, so that other Digimap users can share it.

Map and Data Collections

Ordnance Survey Collection †
Contemporary Ordnance Survey maps and map data.
More information

Historic Digimap †
Historical Ordnance Survey maps from 1843 to 1996.
More information

Geology Digimap †
(Access denied, subscription required)
Current British Geological Survey map data and Lexicon of named Rock Units.
More information

Marine Digimap †
(Access denied, subscription required)
Hydrographic and marine data from SeaZone Solutions Ltd.
More information

Find and Share

Go-Geo! †
Search for geospatial data, information and services.
More information

ShareGeo (Beta) ‡
Find, contribute and share geospatial data with others.
More information

GeoDoc †
Create geospatial metadata for publication in Go-Geo!.

Tools/Developer's Area

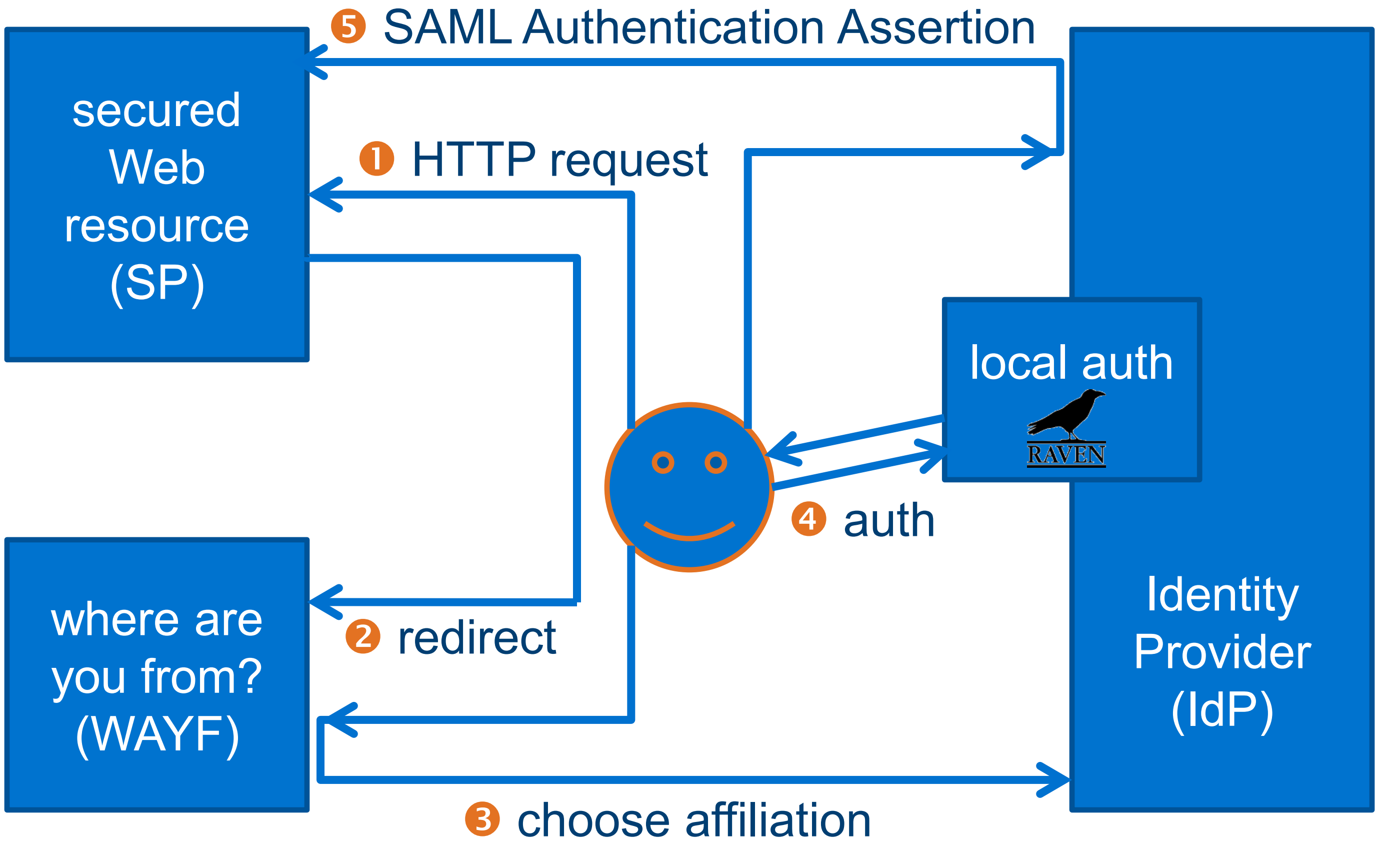
This is a new area which will be available in the near future.
In the meantime, find out about the GeoCrossWalk gazetteer and Digimap mapping APIs in the Ordnance Survey Collection. Separate registration will be required in order to use these.

JISC † JISC funded ‡ JISC supported

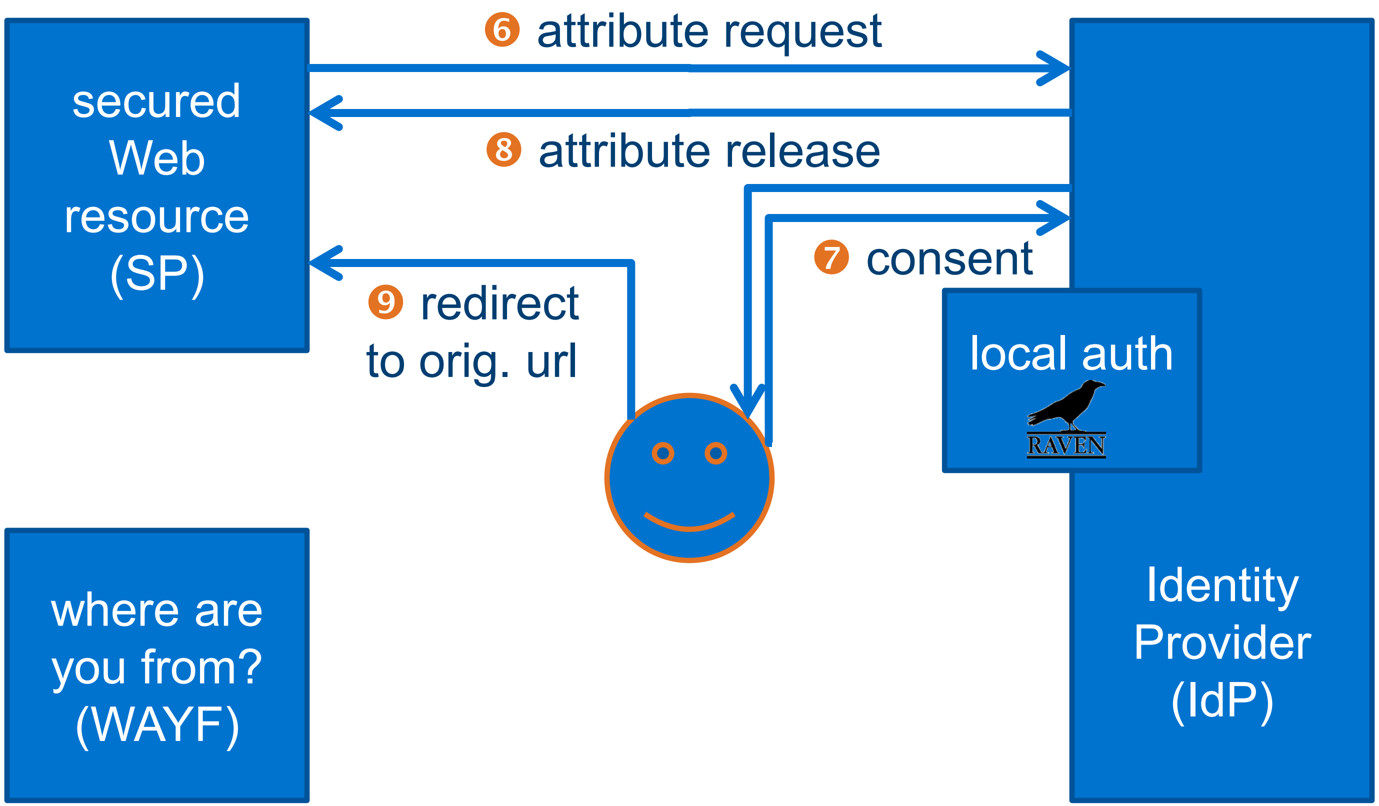
© University of Edinburgh.

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

Shibboleth interaction revisited: authentication



Shibboleth interaction revisited: authorisation



❻ attribute request

❽ attribute release

❼ consent

❾ redirect to orig. url

secured Web resource (SP)

local auth

RAVEN

Identity Provider (IdP)

where are you from? (WAYF)

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

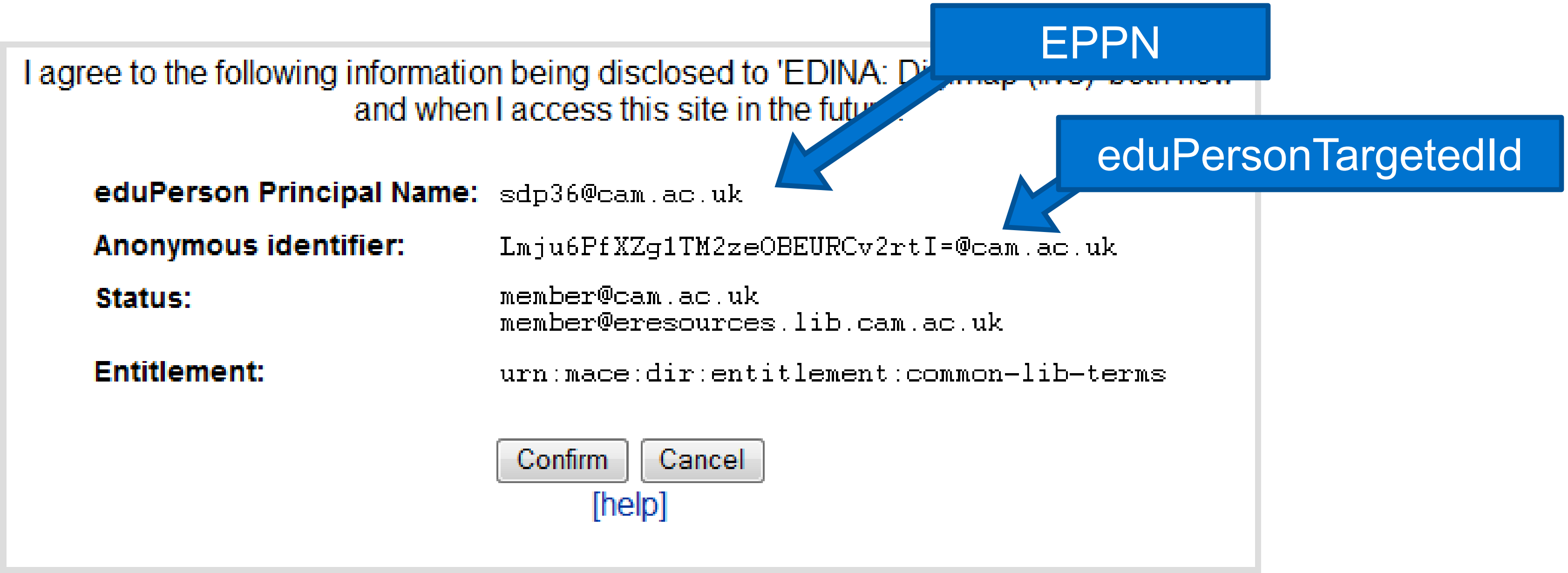
1	what, why, when: Shibboleth basics
2	how: Interaction scenarios
3	**who: privacy issues**
4	whoops: pitfalls and hints

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: Di... both now and when I access this site in the futu...

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

EPPN

eduPersonTargetedId

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
eppn: 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

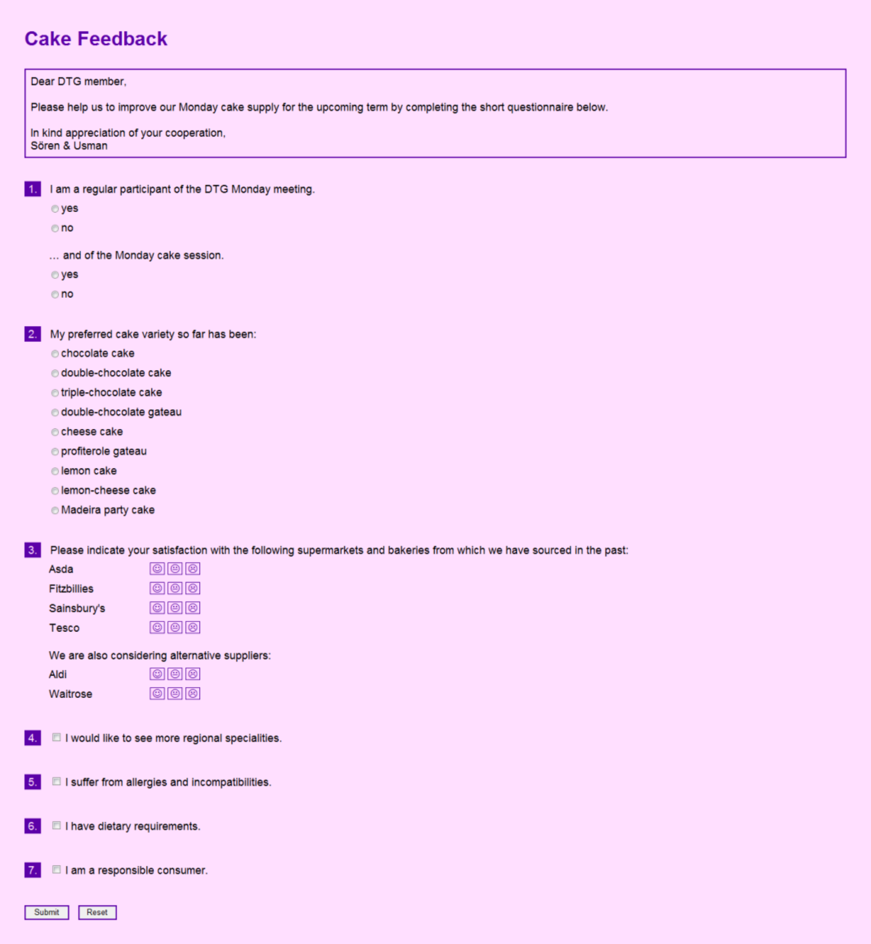
1 what, why, when: Shibboleth basics

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

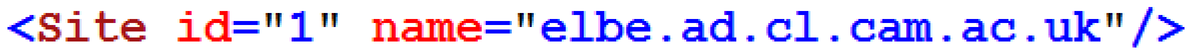
- installing Raven on IIS 7 will mess up the system

- 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

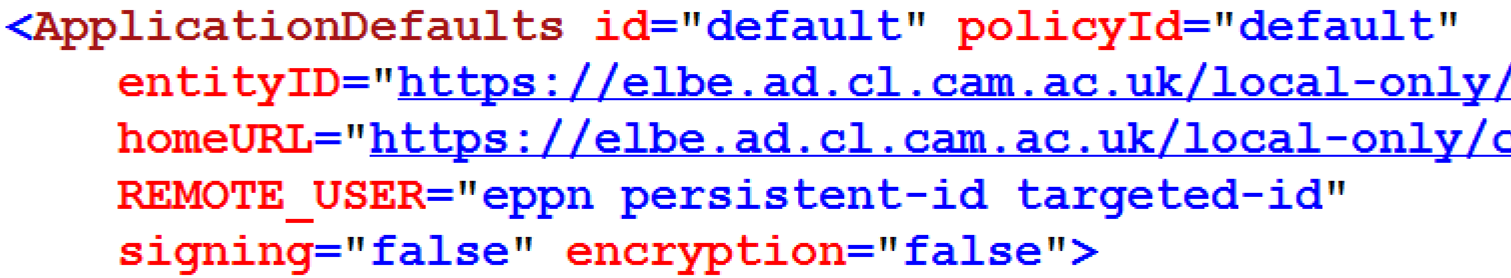
Configuring Shibboleth

- XML configuration files, pre-configured by UCS
- Server details:



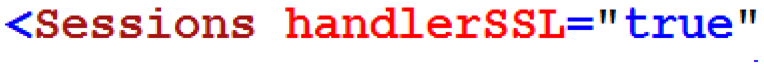
```
<Site id="1" name="elbe.ad.cl.cam.ac.uk"/>
```

- 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/c
        REMOTE_USER="eppn persistent-id targeted-id"
        signing="false" encryption="false">
```

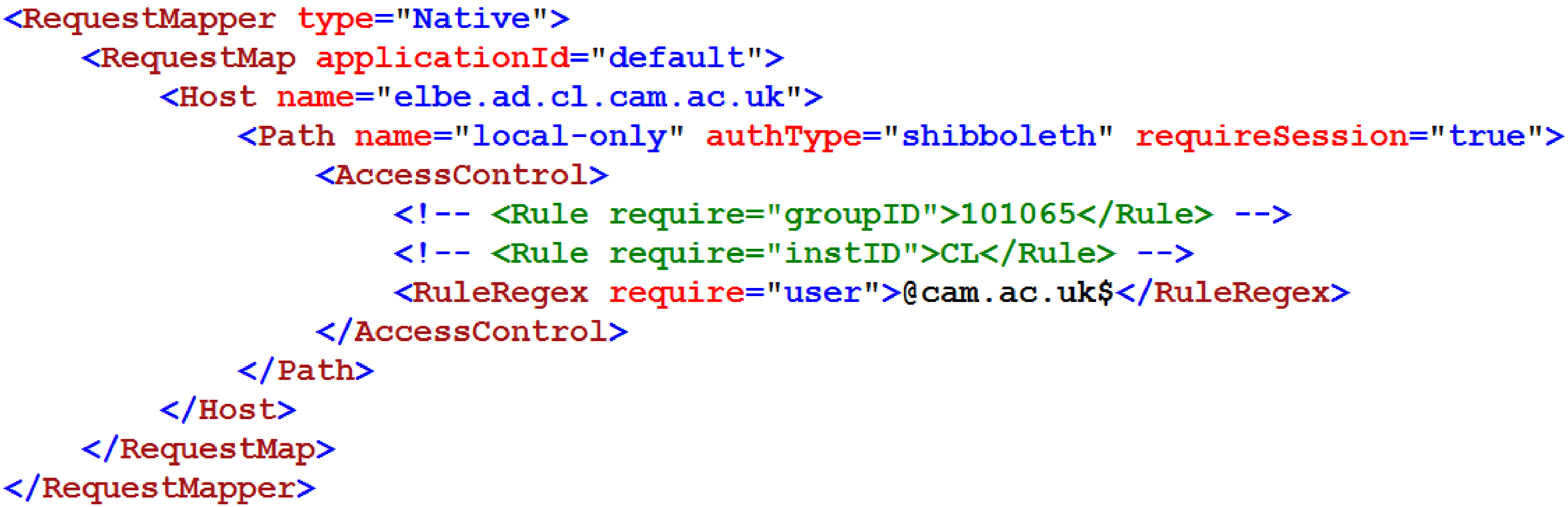
- SSL:



```
<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 expresssions:
  `<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
- "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