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

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

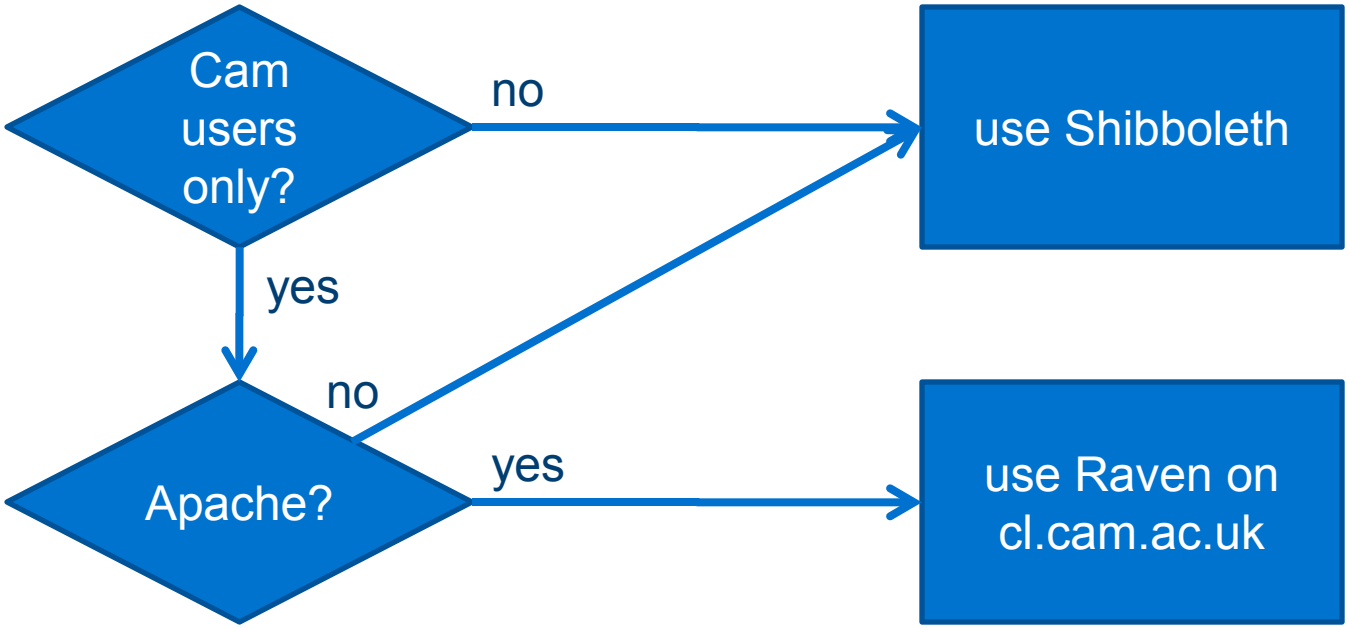
- Authentication and authorisation system for Web resources

- Similar to Raven, but
  - standardised
  - globally cross-organisational
  - successor to Athens (funding stopped June 2008)
  - perceivedly slower

- cf. eduroam

Why and when

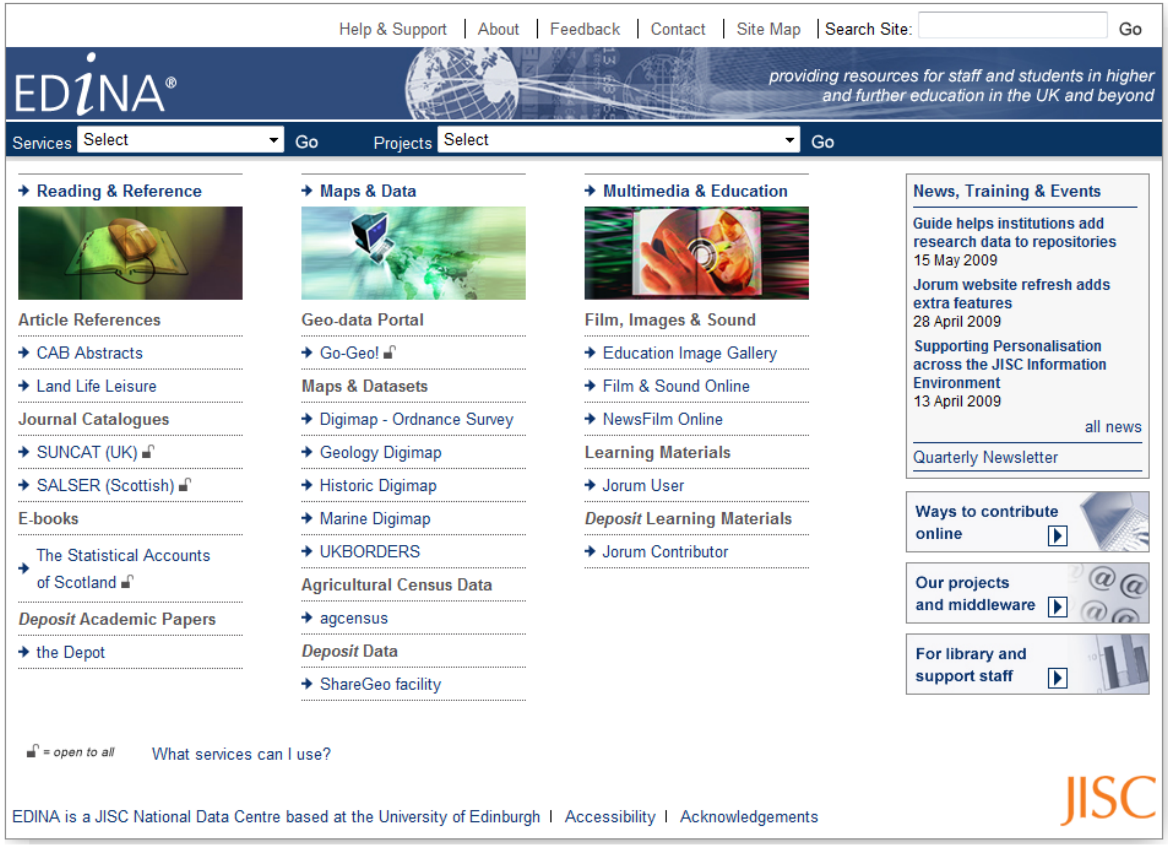
- authenticate people – not IP addresses
- do not proliferate authentication systems



Agenda

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

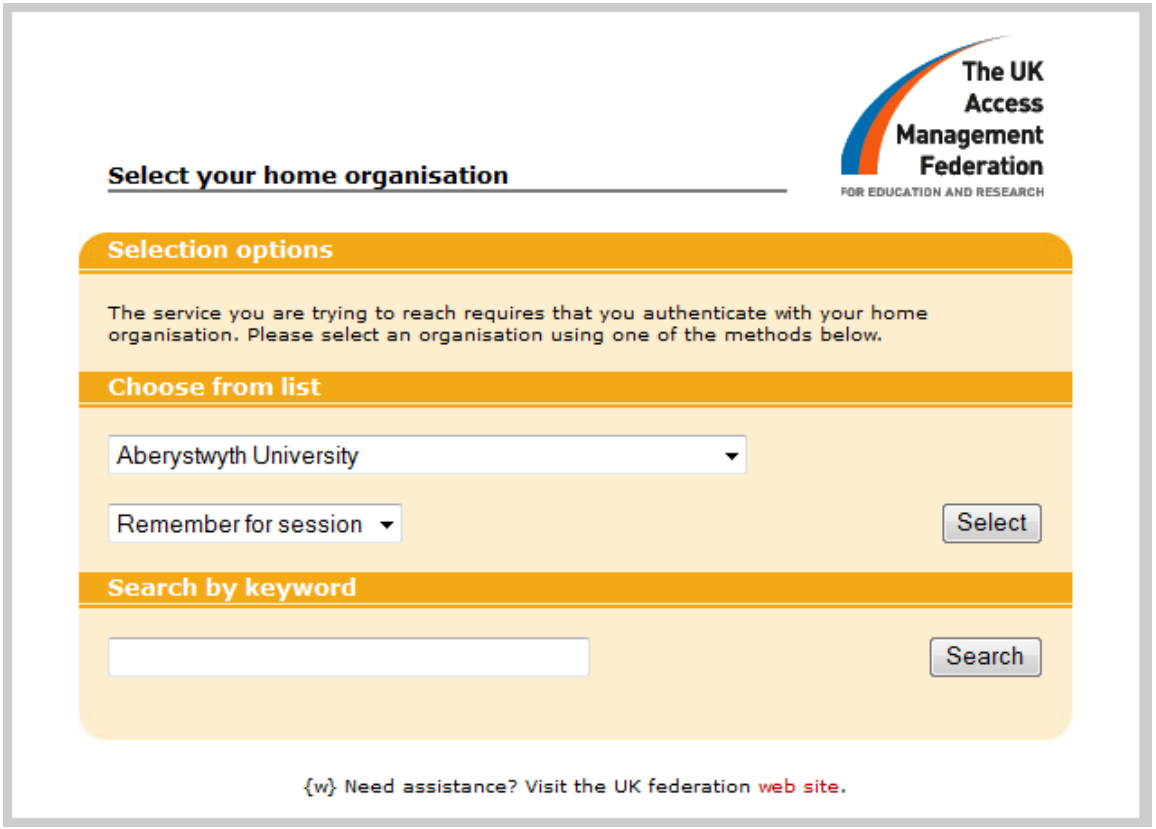
Example: Shibboleth authentication (1)



Example: Shibboleth authentication (2)

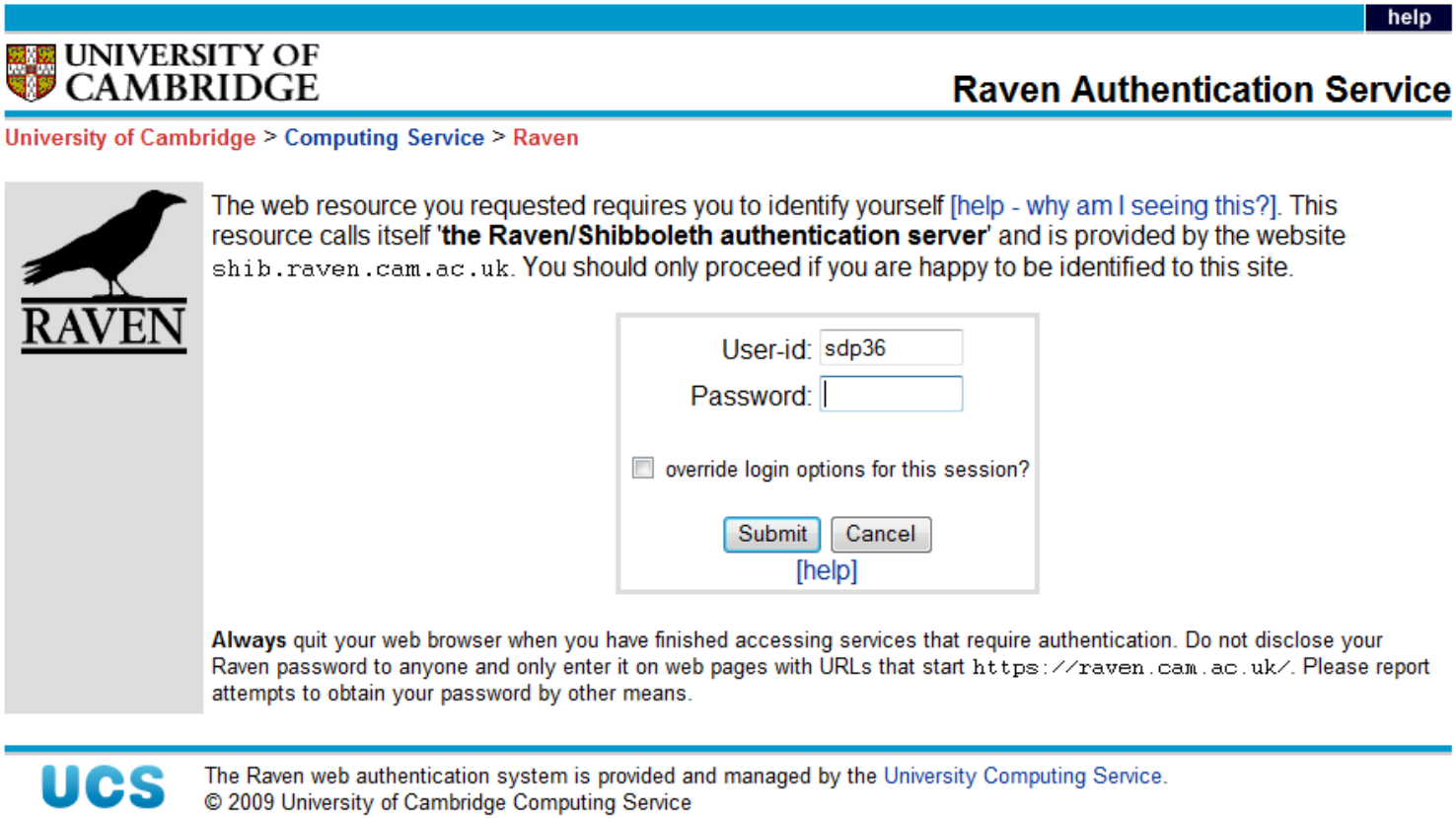
invitation to login

Example: Shibboleth authentication (3)



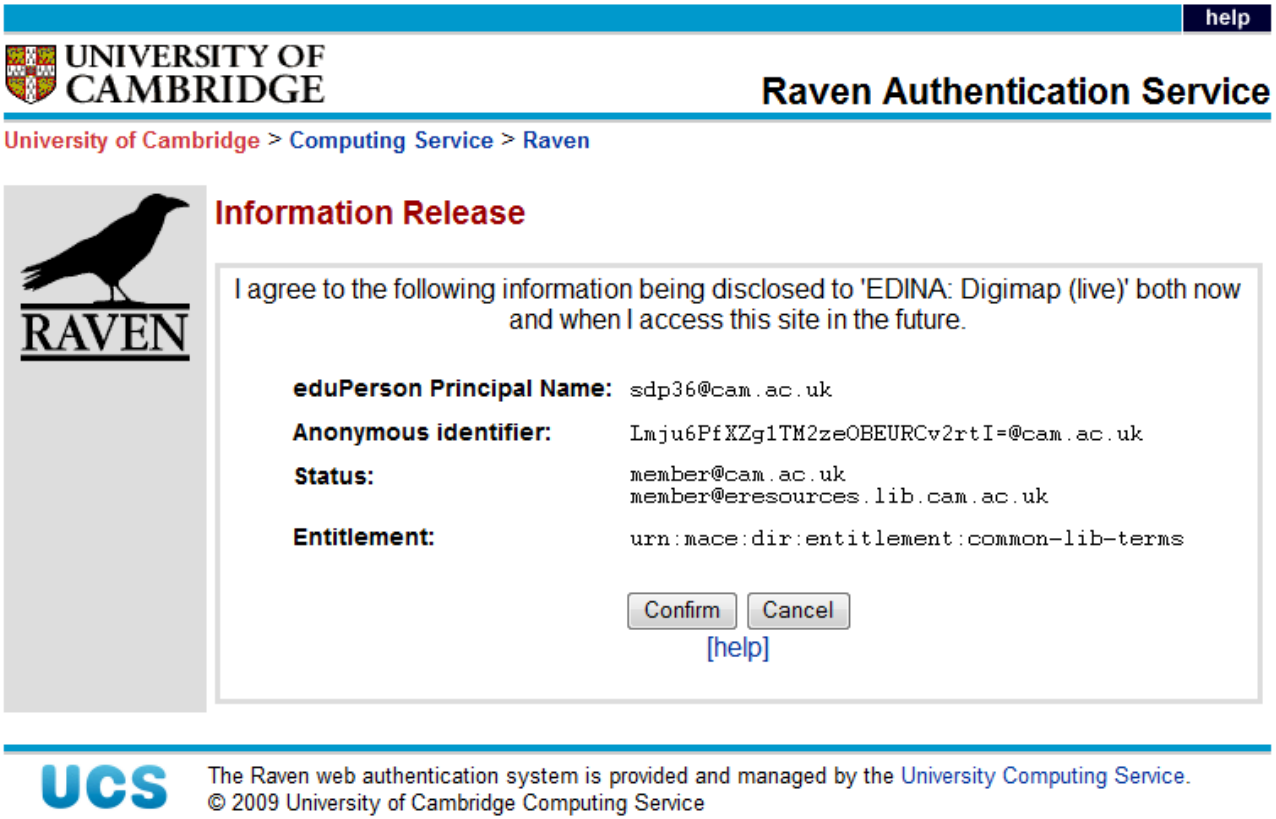
https://wayf.ukfederation.org.uk/shibboleth-wayf/...

Example: Shibboleth authentication (4)



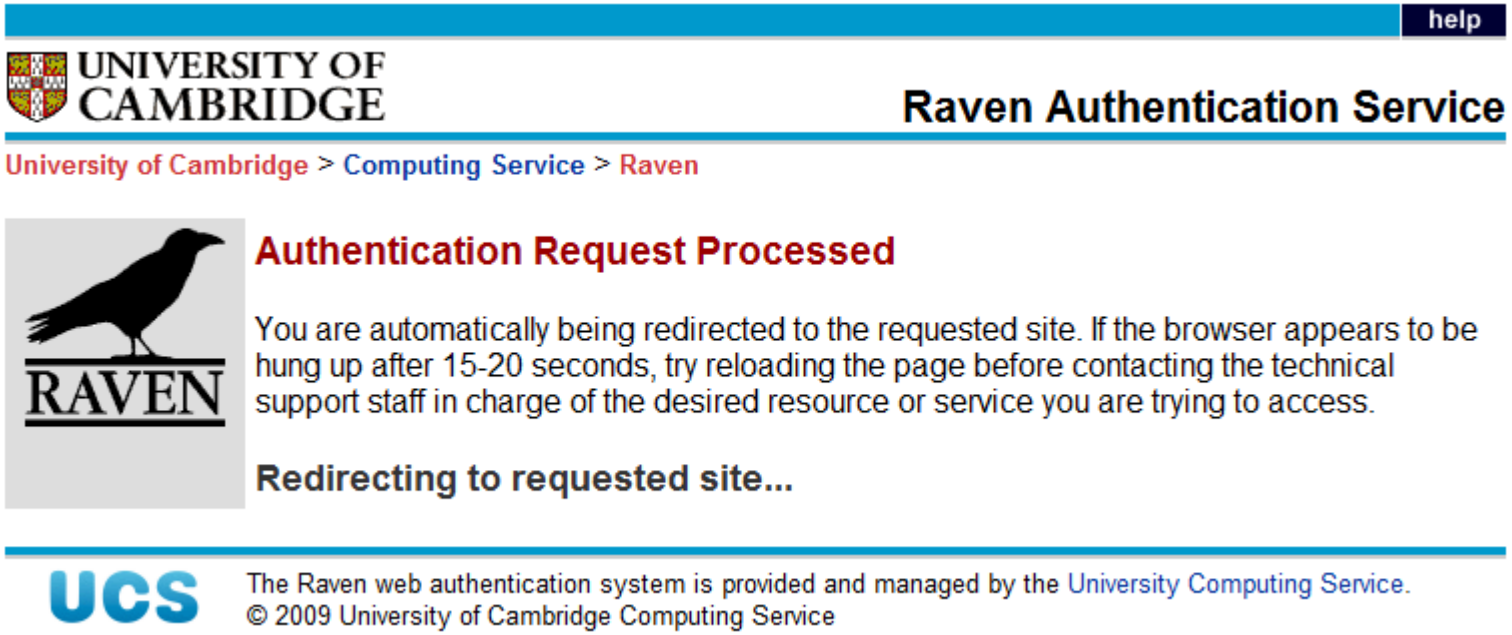
https://raven.cam.ac.uk/auth/authenticate.html?...

Example: Shibboleth authentication (5)



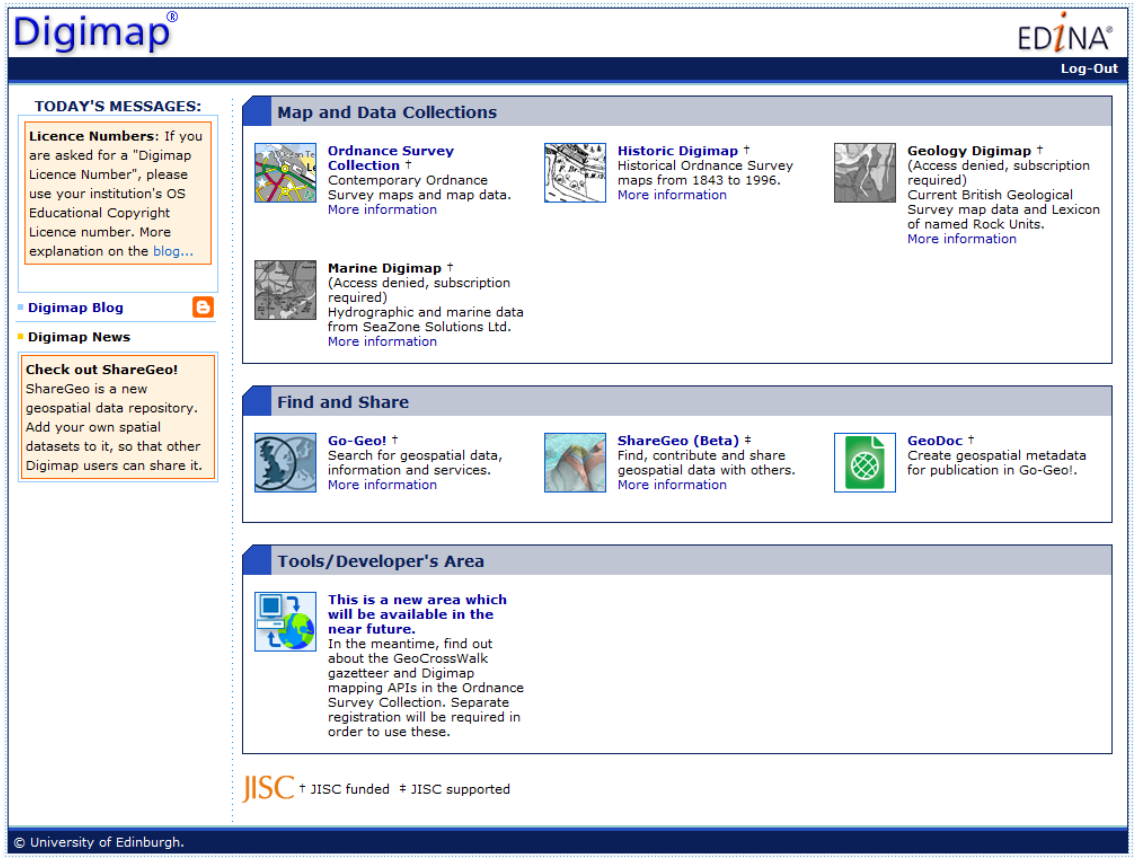
https://shib.raven.cam.ac.uk/arpviewer/...

Example: Shibboleth authentication (6)



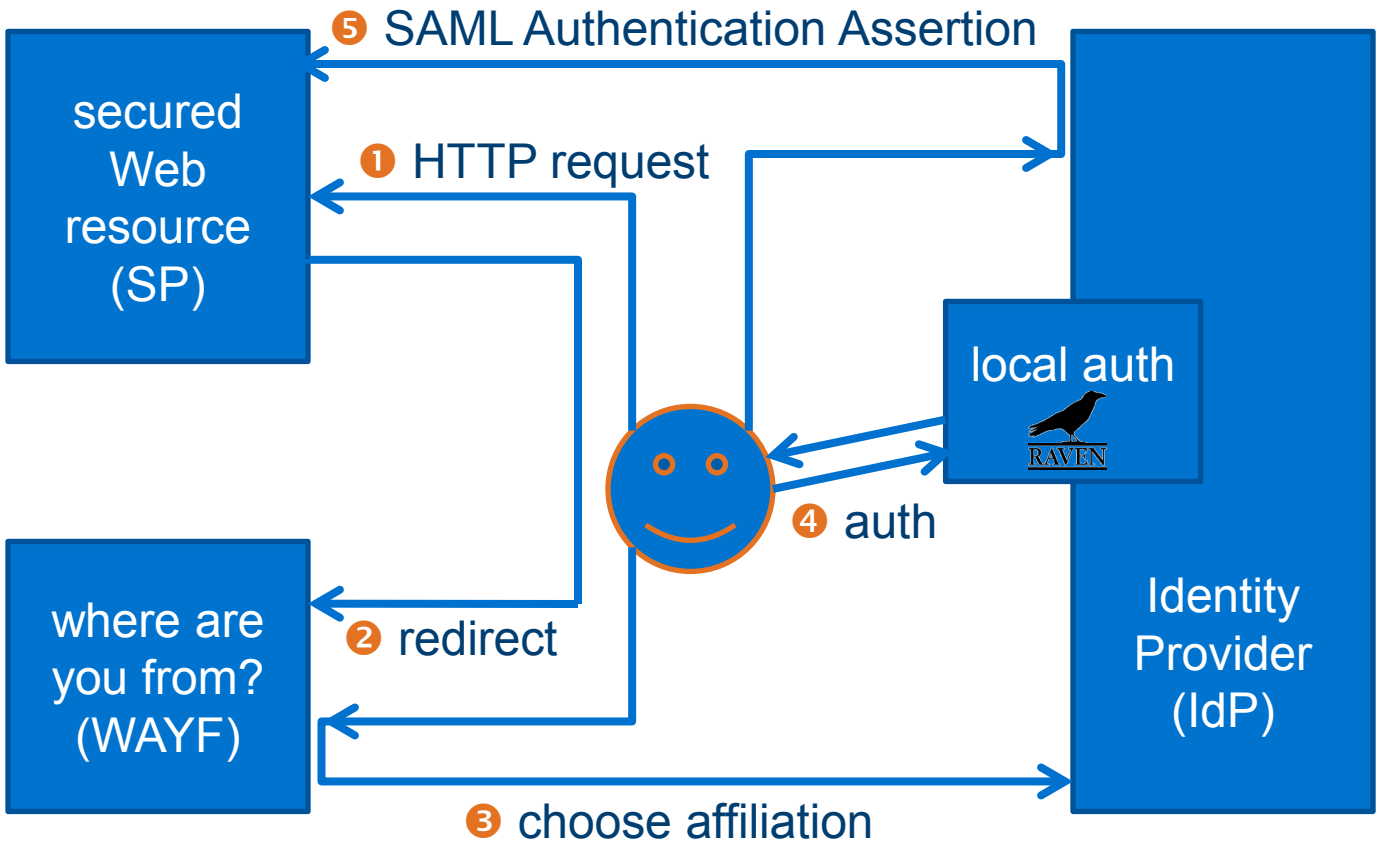
https://shib.raven.cam.ac.uk/shibboleth-idp/...

Example: Shibboleth authentication (7)

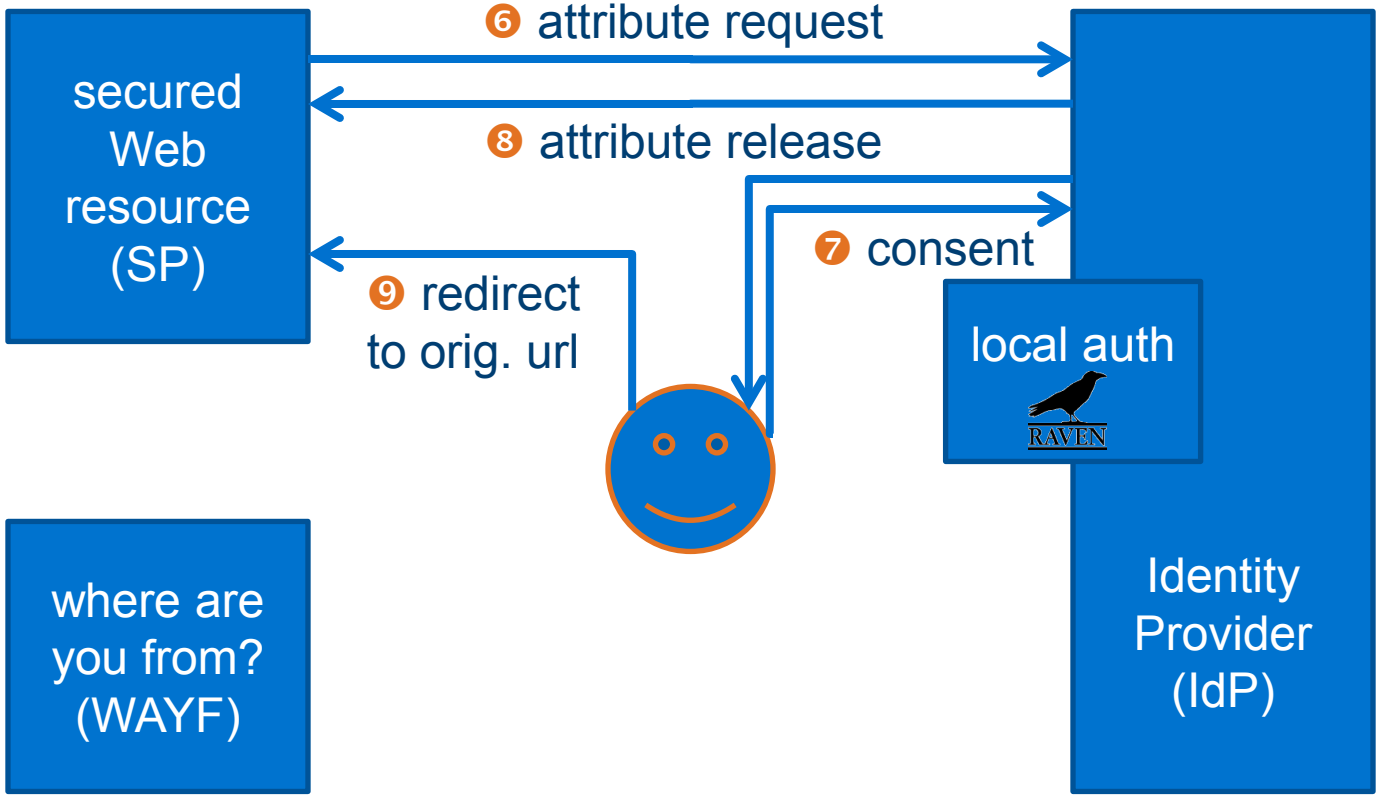


http://digimap.edina.ac.uk/

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

Ucam federation attribute release

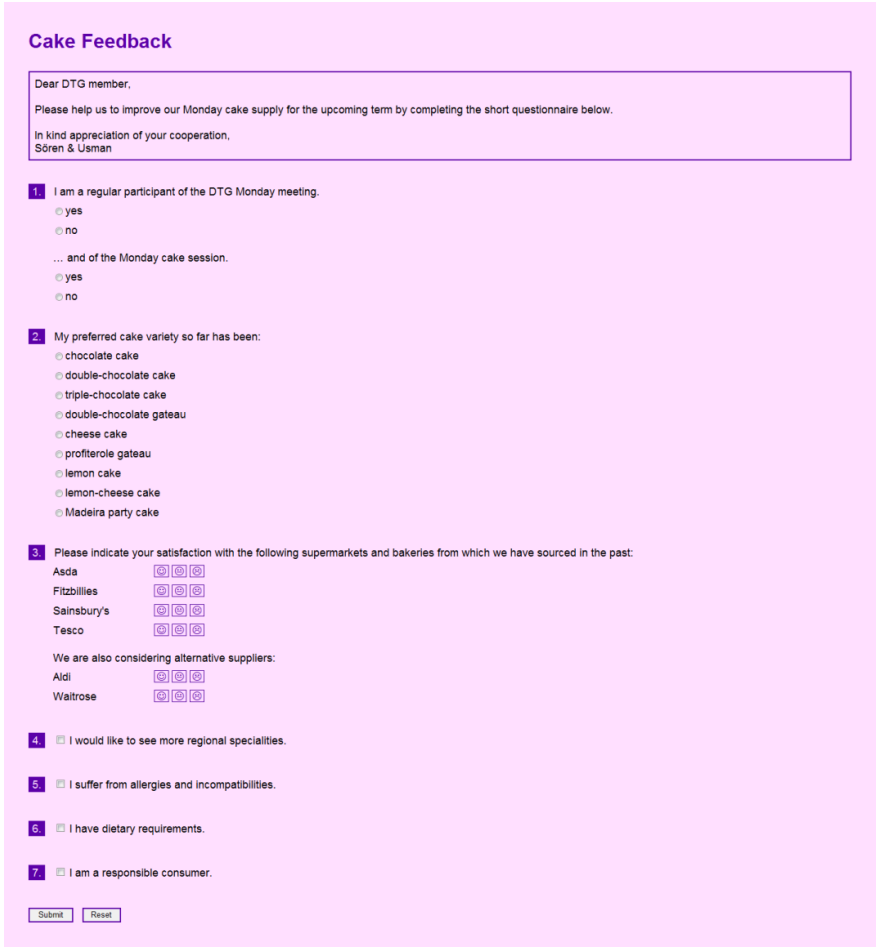
Shib-Application-ID: default
Shib-Session-ID: _c0582d05b229d54d085a14fb74ee1003
Shib-Identity-Provider: https://shib.raven.cam.ac.uk/shibboleth
Shib-Authentication-Instant: 2009-05-18T11:36:59.165Z
Shib-Authentication-Method: urn:oasis:names:tc:SAML:1.0:am:unspecified
Shib-AuthnContext-Class: urn:oasis:names:tc:SAML:1.0:am:unspecified
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.

Submit Reset

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