

# Introducing



**Shibboleth.**

“Then said they unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right. Then they took him, and slew him at the passages of Jordan: and there fell at that time of the Ephraimites forty and two thousand.” (Judges 12:5-6, KJV)

# I keep six honest serving men...

- What?
- Why?
- When?
- How?
- Where?
- Who?

# I keep six honest serving men...

- What ... is it?
- How ... does it work?
- Why ... should we bother?
- When ... is it all going to happen?

*Where and Who are on holiday*

So, what is it?

*“Now here's the thing. As things go, it's not a big thing.  
But it's a thing that's good to know”*

# Officially...

“Shibboleth is an initiative to develop an open, standards-based solution to the needs for organizations to exchange information about their users in a secure, and privacy-preserving manner.”

<http://shibboleth.internet2.edu/shib-intro.html>

(emphasis mine)

# In practice...

- Another authentication/authorisation system for web applications
- A bit like Raven, except
  - standardised
  - designed for deployment on a national or international scale
  - more complicated
  - but from a user's point of view, much the same
- Let me show you...



# Film & Sound Online

## Main Menu

- » Login
- » Description
- » Access to service
- » Help and Support
- » Training and Events
- » Terms of Use
  
- » EDINA Home

You are here: Film & Sound Online

## Login to Film & Sound Online

Film and sound for download. For UK HE and FE.

Cambridge University has direct access to this service.

Please note that access to the medically-restricted Film & Sound Online material is via personal accounts only.

**Login** → via Athens. [\[info\]](#)

**Login** → via direct access. [\[info\]](#)

**Login** → via UK Federation. [\[info\]](#)

## 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

University of Cambridge (pilot) ▼

Remember for session ▼

Select

### Search by keyword

Search

Need assistance? Visit the UK Federation [web site](#).





The web resource you requested requires you to identify yourself [\[help\]](#). This resource calls itself '**the University pilot Shibboleth service**' 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.

[Home](#)[Advanced Search](#)[Collections](#)[Subjects](#)[Search History](#)[Help | Exit](#)

## SEARCH

Search for (see example):

in

## SHOWCASE

**“One of the finest ethnographic film collections that document Himalayan cultures”**

*Digital Himalaya project team, University of Cambridge*



**Title:** Nepal, Sherpa (3)

**Collection:** Digital Himalaya

## BROWSE

■ [Browse by collections](#) →

■ [Browse by subjects](#)



[Culture](#)



[Education](#)



[Country & Information](#)



[Country & Groupings](#)  
[Communication](#)



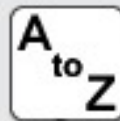
[Politics, Law & Economics](#)



[Science](#)



[Social & Human Sciences](#)



[A to Z](#)

**LUCKY DIP** →

[Keep in touch with service developments](#) →

[View or create learning materials](#) →

All images © JupiterImages 2006

[Terms of Use](#)[FAQs](#)[Accessibility](#)

# Internet2's initiative

- To support sharing – between domains – of secured web resources and services
- Delivering:
  - an architecture and policy framework
  - a set of SAML profiles
  - an open source implementation  
(<http://shibboleth.internet2.edu/>)
- There is at least one other open source implementation: Guanxi  
<http://www.guanxi.uhi.ac.uk/index.php/Guanxi>About>

# Some things it isn't

- A Web Single Sign On (SSO) system
- An access control system for information
- A standard vocabulary for information
- A standard for adding AuthN and AuthZ to applications

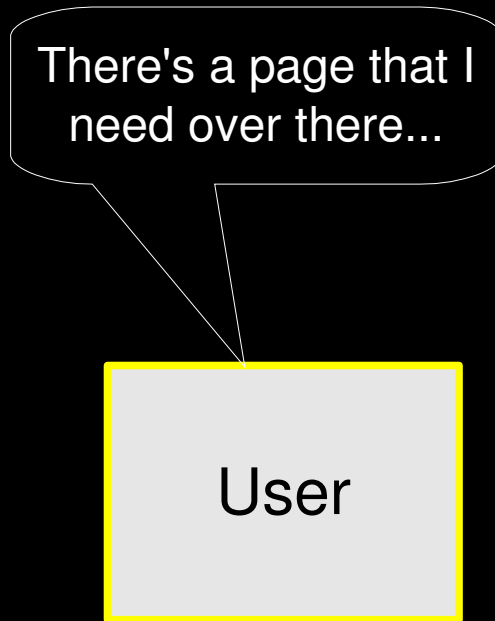
... but it just might be a way of binding  
all these together

# A word or two on terminology

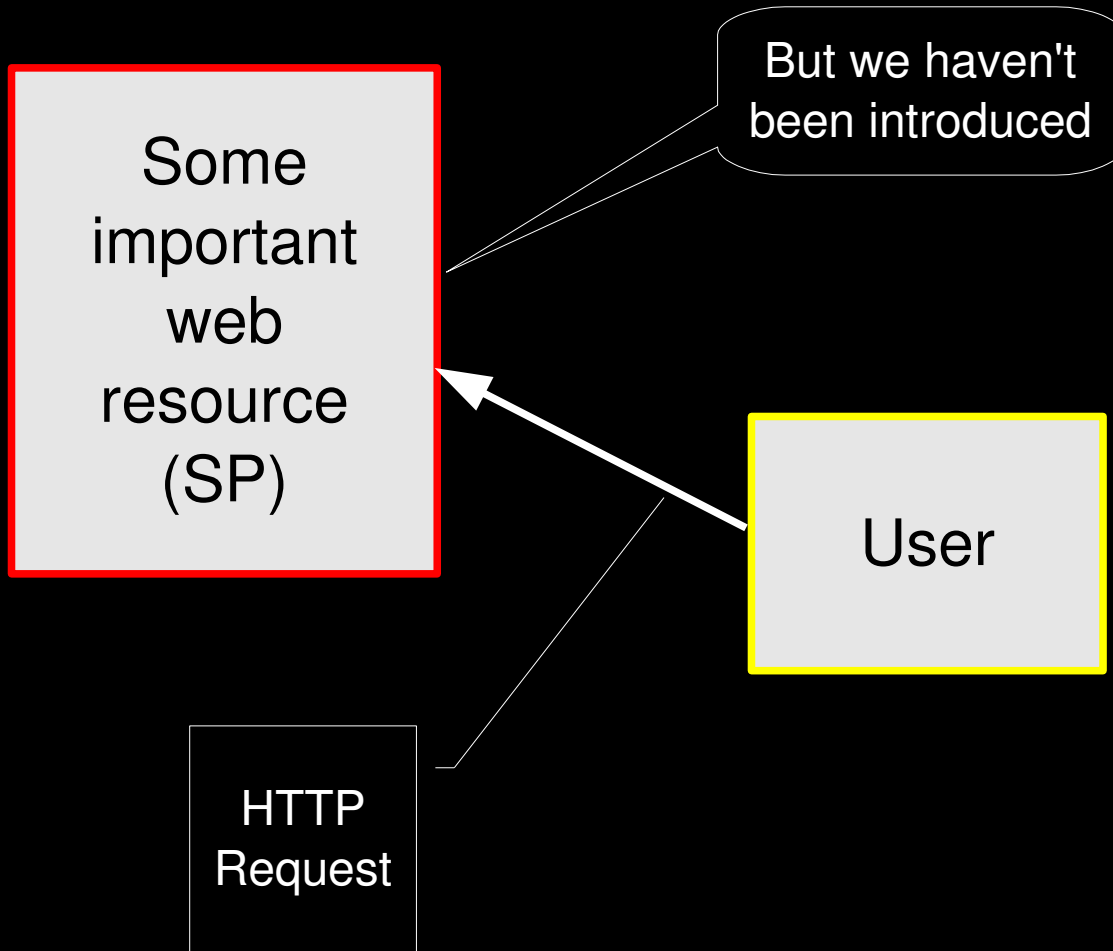
- UcamWebauth
  - The protocol currently used with Raven
- Shibboleth
  - Another protocol (for want of a better term)
- Raven
  - an authentication service
  - which supports UcamWebauth and Shibboleth authentication

How does it work?

# How does it work?

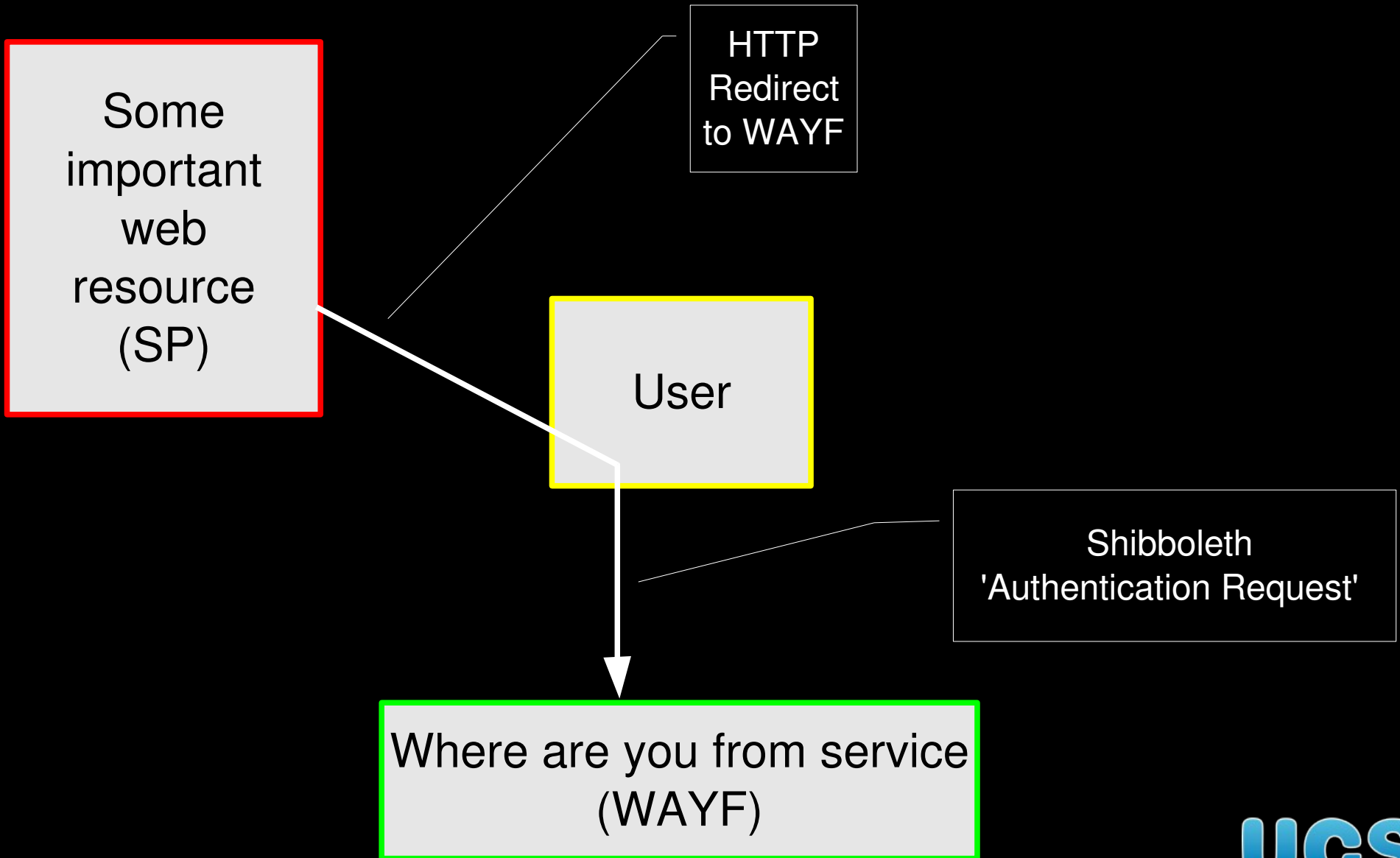


# How does it work?

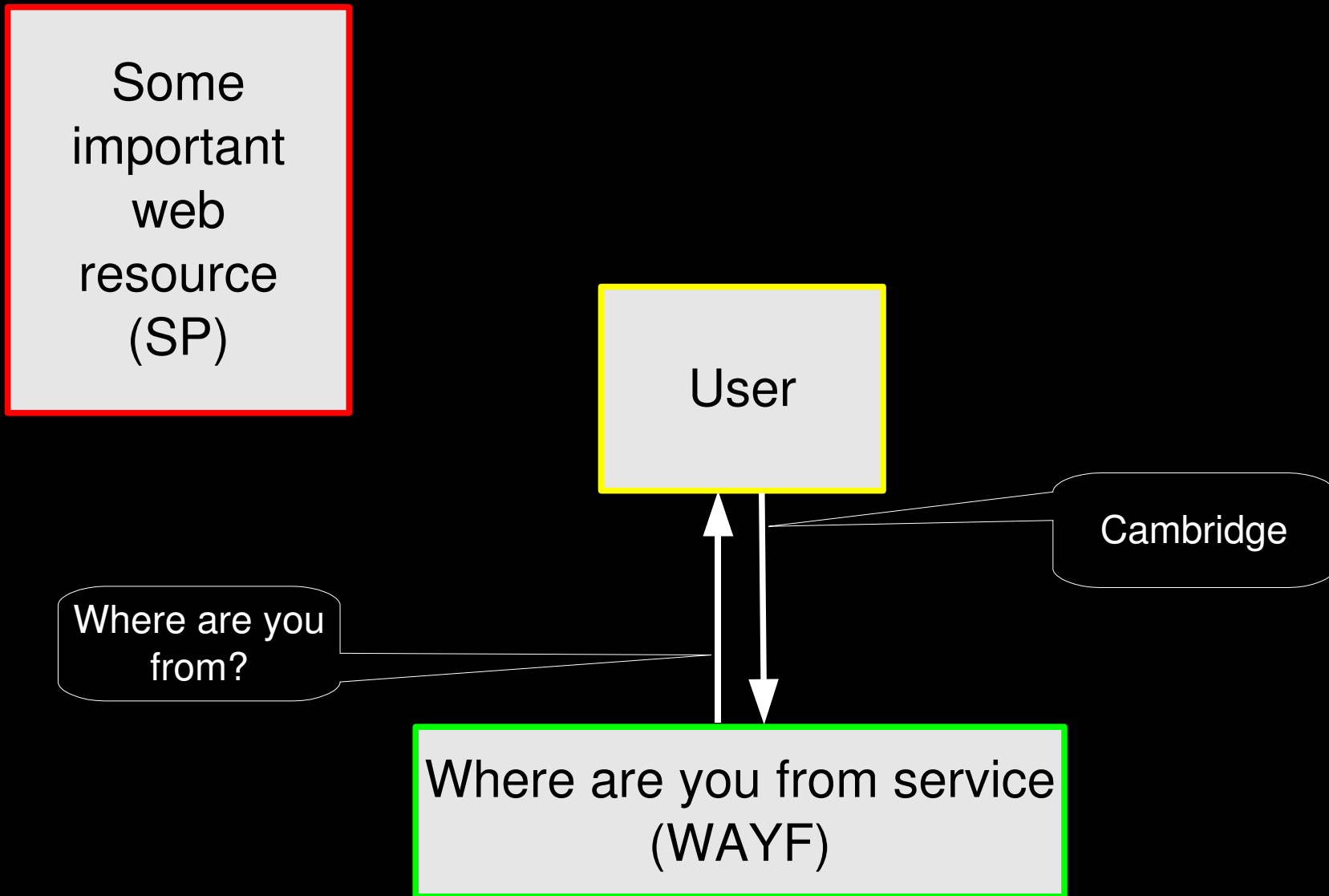




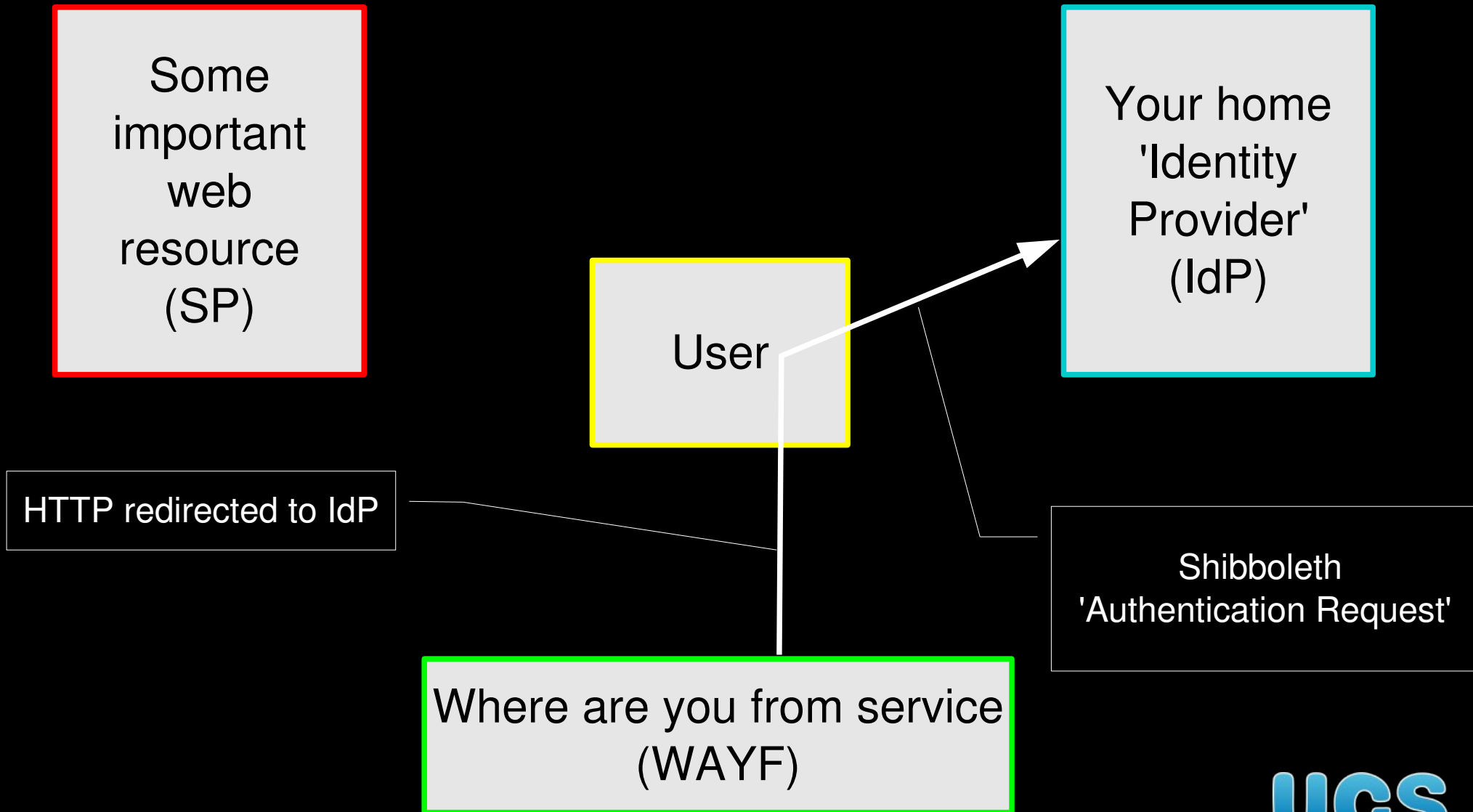
# How does it work?



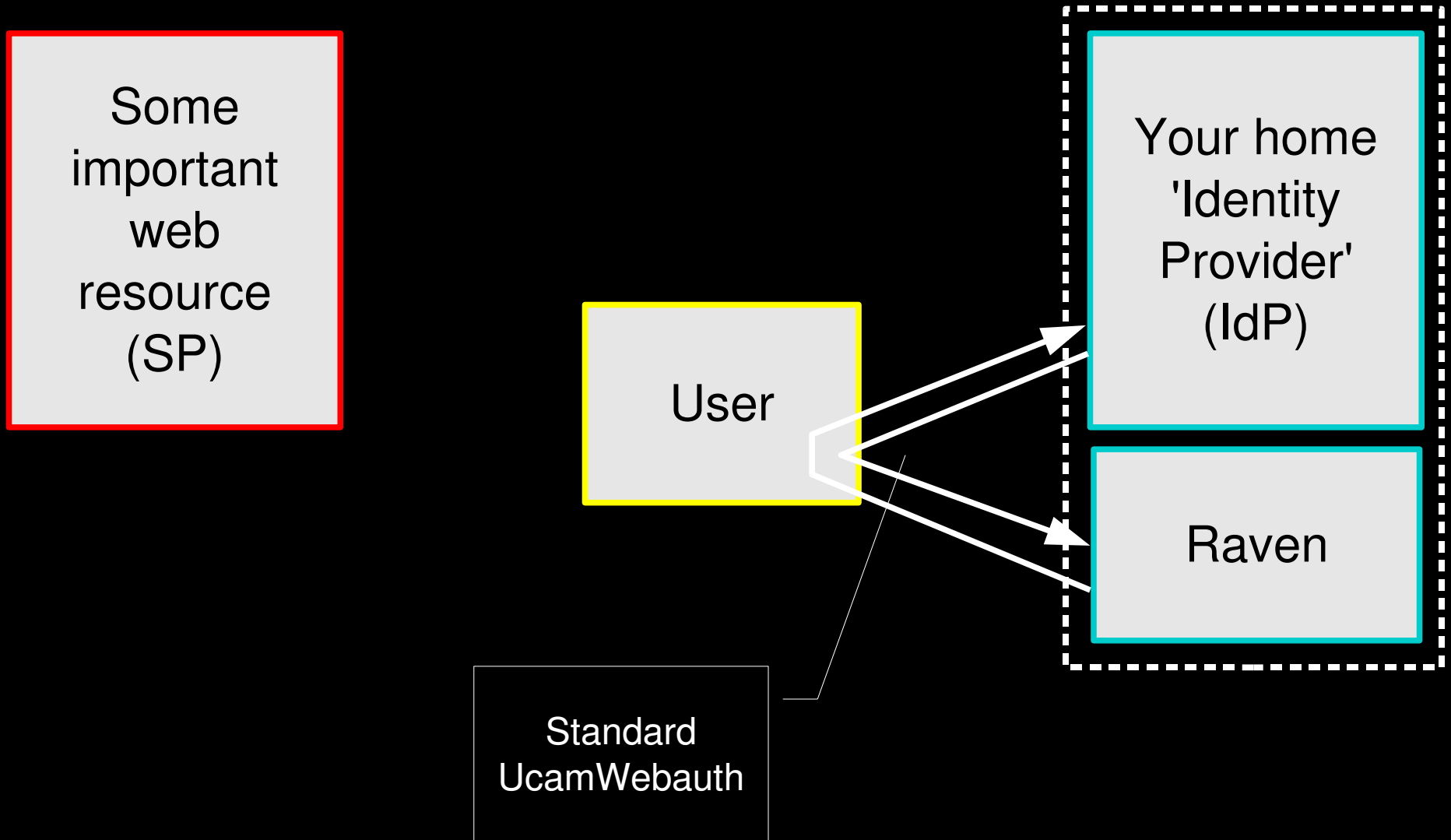
# How does it work?



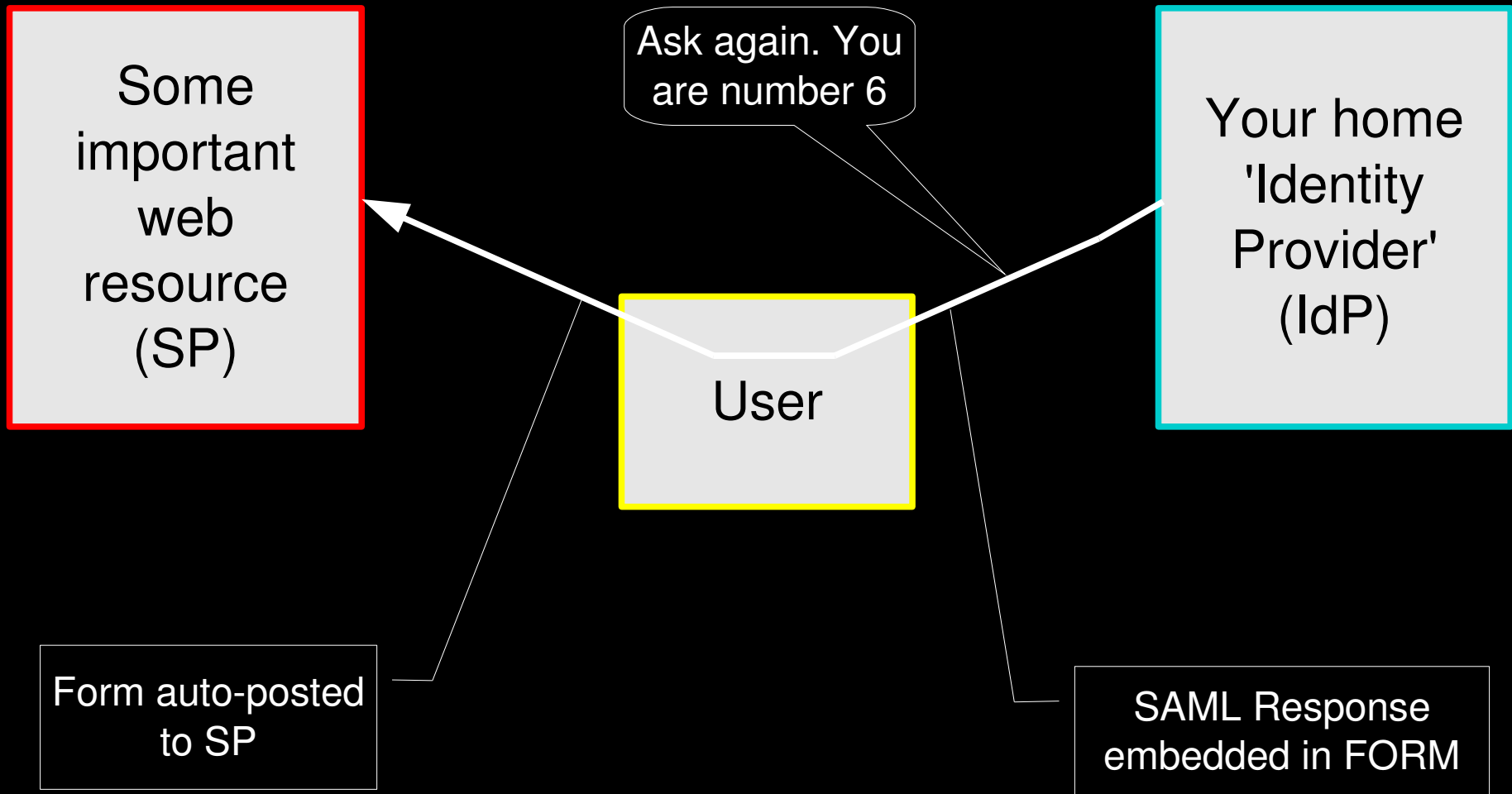
# How does it work?



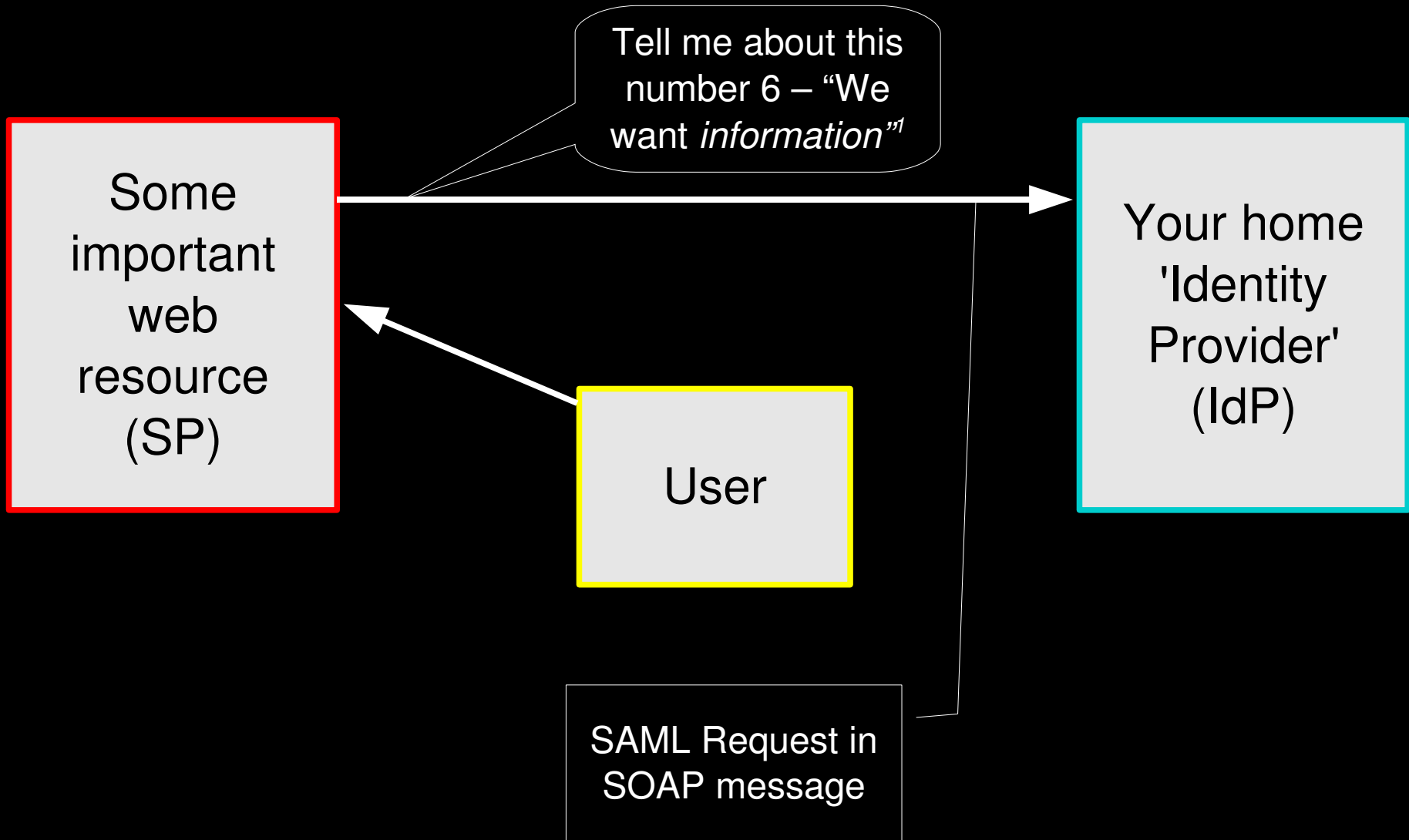
# How does it work?



# How does it work?

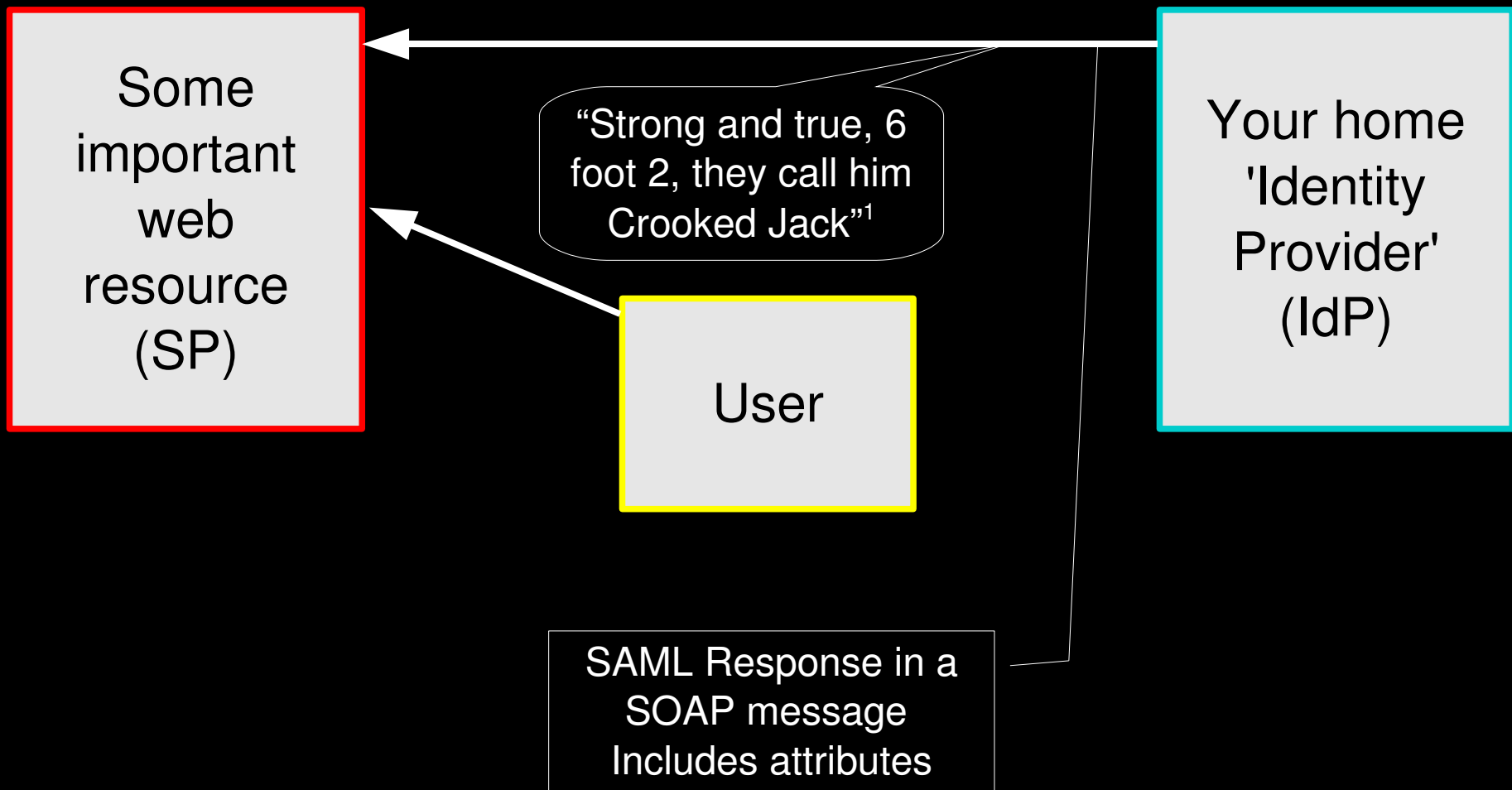


# How does it work?



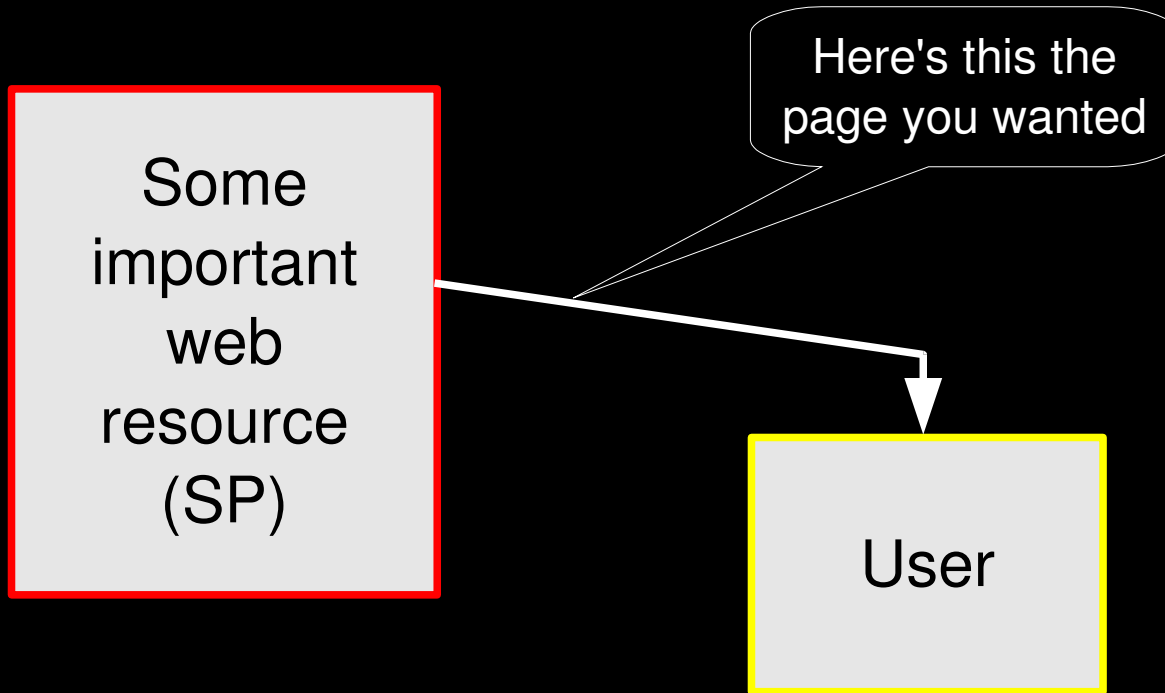
<sup>1</sup> "The Prisoner", ITC Entertainment, 1967

# How does it work?



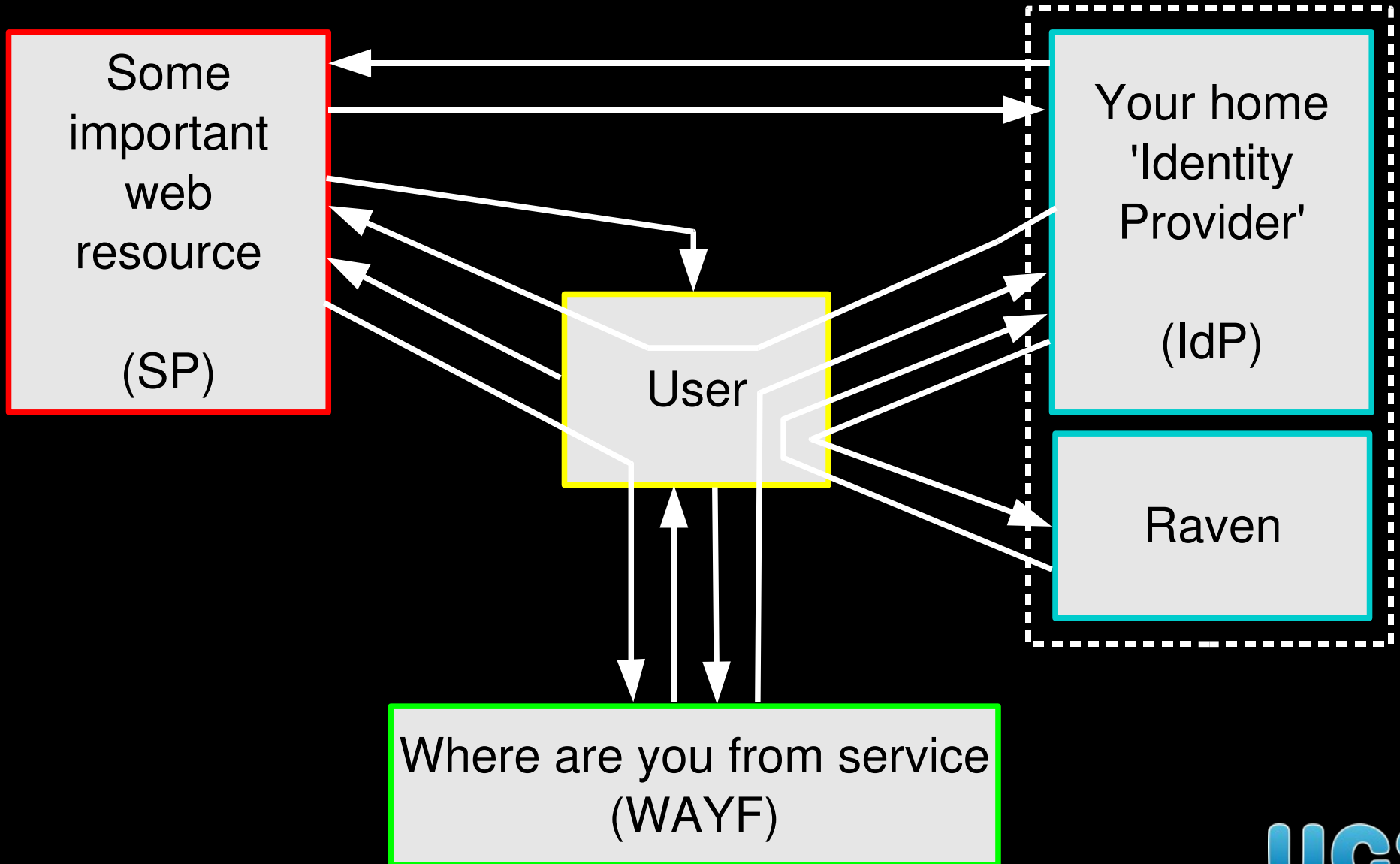
<sup>1</sup> Bodega (<http://www.bodegaband.com/>), "Crooked Jack"

# How does it work?





# How does it work?




# Small things worth noting

- Lots of crypto
- Further requests are quicker
- That was “SP first” - “IdP first” is also possible
- That was Browser/POST; there's also Browser/Artefact
- The WAYF can be provided by the SP
- Use of SAML (but SAML *isn't* Shibboleth)

[Home](#)[Browse](#)[Search](#)[My Settings](#)[Alerts](#)[Help](#)**Quick Search**

Title, abstract, keywords

Author

 [search tips](#)

Journal/book title

Volume

## Login via Athens or Your Institution

You may be able to login to ScienceDirect using Athens or your institution's login credentials. You can also choose to remember your login preference the next time you access ScienceDirect from this machine.

**If you are an Athens user, please select the link below.**

[Athens Login](#)

**To login using your institution's login credentials, select a region or group.**

UK Higher &amp; Further Education (SDSS)

[View All Institutions](#)

Please choose one of the institutions listed below:

If your institution is not listed, it is not enabled for this type of login. Please contact your Librarian or Information Specialist.

### UK Higher & Further Education (SDSS)

- [JISC Project: Angel](#)
- [London School of Economics and Political Science](#)
- [Oxford University Computing Services \(Test\)](#)
- [SDSS](#)
- [University College London](#)

# Federated authentication

- User authenticates at their 'home institution'
  - rather assumes that they only have one...
- Using password + system that they already know
- Re-uses existing systems – in theory only a little more work

# Role-based authentication

- Attributes transferred from IdP to SP
- May or may not include real-world identity
  - supports privacy (good for users)
  - reduces data protection issues (good for SPs and IdPs)
- Non-anonymous attributes also supported
- Many attributes based on existing LDAP schema, but this isn't required

# Federations

- Many things need to be agreed between IdPs and SPs. In particular trust.
- Doesn't scale if done bilaterally
- 'Federations' address this
  - “UK Access Management Federation for Education and Research” (JISC, BECTA) (<http://www.ukfederation.org.uk/>)
  - InCommon (Internet2, US)
  - Others (Australia, Belgium, Finland, France, Germany, Netherlands, Norway, Sweden, Switzerland, ...)

# UK federation core attributes

- eduPersonScopedAffiliation
  - member@cam.ac.uk
- eduPersonTargetedID
  - 12765988765438424418@cam.ac.uk
- eduPersonPrincipalName
  - jw35@cam.ac.uk
- eduPersonEntitlement
  - urn:mace:ac.uk:sdss.ac.uk:entitlement:emol.sdss.ac.uk:restricted

# UK Federation core attributes

**Scoped Affiliation:** member@cam.ac.uk

**eduPerson Principle Name:** jw35@cam.ac.uk

**eduPerson Entitlement:**

**eduPerson Targeted ID (old):** MIWd0XIR7juZvwvarOVdYiUWPW0=@cam.ac.uk

**eduPerson Targeted ID (new):** <https://shib.raven.cam.ac.uk/shibboleth!https://mnementh.csi.cam.ac.uk/shibboleth>

## Other attributes used by UK Federation members

**Given Name:**

**Surname:** Warbrick

**Organisational Unit:** University Computing Service

**e-mail:** jw35@cam.ac.uk

## Other attributes from *lookup*

**Common Name:** J. Warbrick

**Display Name:** Jon Warbrick

**Lookup Group:** 100656;100668



# Metadata

```
<EntityDescriptor ID="uk000203" entityID="https://shib.raven.cam.ac.uk/shibboleth">
  <!--
    This is a test IdP for the University of Cambridge.
  -->
  <Extensions>
    <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0" regexp="false">cam.ac.uk</shibmeta:Scope>
    <UKFederationMember xmlns="http://ukfederation.org.uk/2006/11/label"></UKFederationMember>
    <AccountableUsers xmlns="http://ukfederation.org.uk/2006/11/label"></AccountableUsers>
  </Extensions>
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">
    <Extensions>
      <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0" regexp="false">cam.ac.uk</shibmeta:Scope>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>shib.raven.cam.ac.uk</ds:KeyName>
      </ds:KeyInfo>
    </KeyDescriptor>
    <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" Location="https://shib.raven.cam.ac.uk:8443/shibboleth-idp/Artifac
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://shib.raven.cam.ac.uk/shibboleth-idp/SSO"></SingleSignOnSer
  </IDPSSODescriptor>
  <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
    <Extensions>
      <shibmeta:Scope xmlns:shibmeta="urn:mace:shibboleth:metadata:1.0" regexp="false">cam.ac.uk</shibmeta:Scope>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>shib.raven.cam.ac.uk</ds:KeyName>
      </ds:KeyInfo>
    </KeyDescriptor>
    <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" Location="https://shib.raven.cam.ac.uk:8443/shibboleth-idp/AA"></Attributes
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
  </AttributeAuthorityDescriptor>
  <Organization>
    <OrganizationName xml:lang="en">University of Cambridge</OrganizationName>
    <OrganizationDisplayName xml:lang="en">University of Cambridge (pilot)</OrganizationDisplayName>
    <OrganizationURL xml:lang="en">http://www.cam.ac.uk</OrganizationURL>
  </Organization>
  <ContactPerson contactType="support">
    <GivenName>Raven Support</GivenName>
    <EmailAddress>mailto:raven-support@ucs.cam.ac.uk</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="technical">
    <GivenName>Jon</GivenName>
    <SurName>Warbrick</SurName>
    <EmailAddress>mailto:jw35@cam.ac.uk</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="administrative">
    <GivenName>Jon</GivenName>
    <SurName>Warbrick</SurName>
    <EmailAddress>mailto:jw35@cam.ac.uk</EmailAddress>
  </ContactPerson>
</EntityDescriptor>
```

Why should we bother?

# “Are we bothered?”

- Inter-institution support
- Already some interest from e.g. e-Science
- Shibboleth is a 'Standard'
  - some open source apps already come with support
- It does *AuthN and AuthZ*
  - intra-institution use?
- But ...

# ... the big driver is Athens

- Currently controlling access to many UL electronic resources (esp. 'off site access')
- A “big database, with 3 million rows and 300 columns”
- Central funding goes away June 2008, Shibboleth and the UK Federation is its intended replacement
  - also Shibboleth-to-Athens gateway
- Shib was designed for this sort of use

# Why replace Athens?

- YAP (yet another password)
- UK only - a problem for vendors
- Cost
- Account management overhead
- Lack of privacy
- But remember: “LIBRARY ELECTRONIC RESOURCES ARE NOT THE ONLY THING SHIBBOLETH CAN BE USED FOR”

# The ~~problems~~ issues

- Data availability
- Data protection
- Staff time (deploy, document, debug, assist)
- User confusion (change, failures, ...)
- SPs slow to adopt Shibboleth
  - Some (Westlaw, Lexis/Nexis) being slow to support even the Shib-to-Athens Gateway

When is it all going to happen?

# Things already have!

- January 2007: Shib project started
- January 2007: UofC joins UK federation
- February 2007: pilot IdP available
- February 2007 onward: press and publicity (Newsletter, IT Liaison, Techlink)



# The future's bright, the future's ...

- March-September 2007: build production IdP
- October 2007: first academic year without full Athens cover
- June 2008: end of Athens - transfer or pay

<https://wiki.csx.cam.ac.uk/raven/Shibboleth>

If you have been, thanks for listening

*“One million Hows, two million Wheres,  
And seven million Whys”<sup>1</sup>*

Any questions?

<sup>1</sup> Kipling, “I keep 6 Honest Serving Men” from “Just So Stories” ([http://www.kipling.org.uk/poems\\_serving.htm](http://www.kipling.org.uk/poems_serving.htm))