Shibbolizing uPortal and a Path for Delegated Authentication with Shibboleth

Tom Barton, Scott Cantor, and Andrew Petro

The Ohio State University, University of Chicago, and Unicon, respectively.

Jasig Dallas
03 March 2009

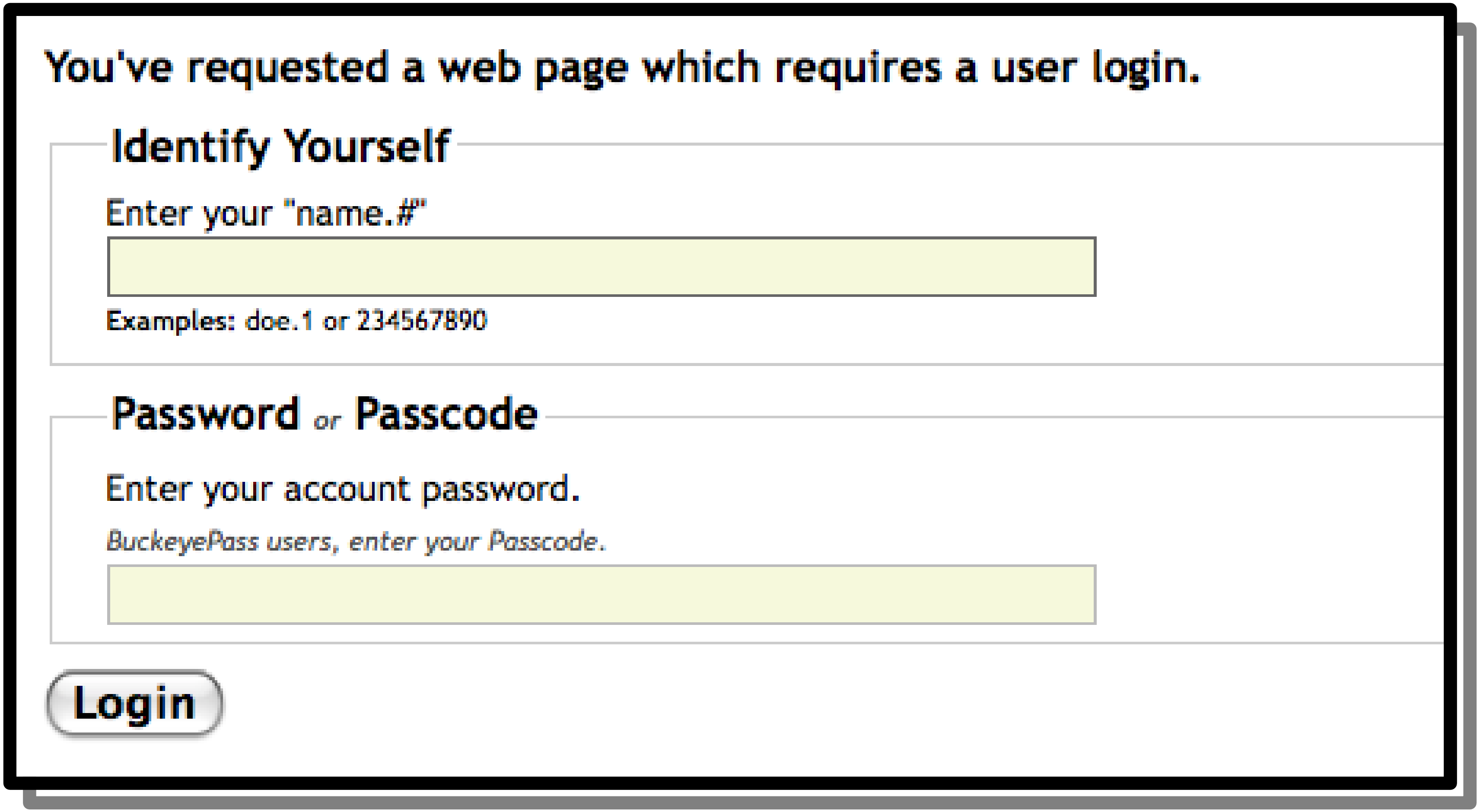
Agenda

1. Introduction
2. Use Cases
3. Shibbolizing uPortal Today
4. Delegated Shibbolized Authentication... in uPortal
5. … in Shibboleth
6. Conclusion

Use Cases

Shibbolizing uPortal

Authentication and Single Sign On



You've requested a web page which requires a user login.

Identify Yourself

Enter your "name.#"

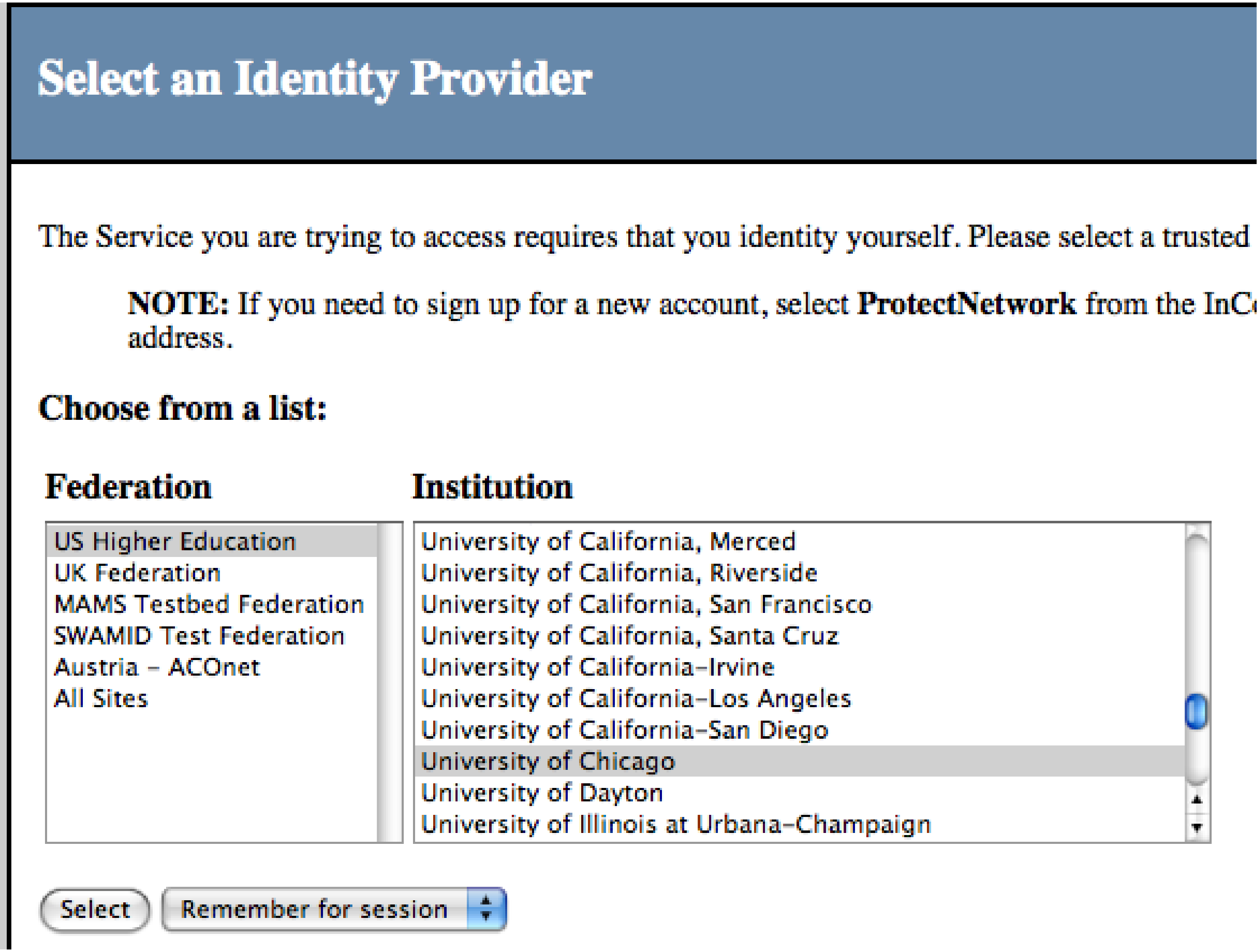
Examples: doe.1 or 234567890

Password or Passcode

Enter your account password.

BuckeyePass users, enter your Passcode.

Federated Authentication



Select an Identity Provider

The Service you are trying to access requires that you identity yourself. Please select a trusted

> **NOTE:** If you need to sign up for a new account, select **ProtectNetwork** from the InC
> address.

Choose from a list:

Federation

- US Higher Education
- UK Federation
- MAMS Testbed Federation
- SWAMID Test Federation
- Austria - ACOnet
- All Sites

Institution

- University of California, Merced
- University of California, Riverside
- University of California, San Francisco
- University of California, Santa Cruz
- University of California-Irvine
- University of California-Los Angeles
- University of California-San Diego
- University of Chicago
- University of Dayton
- University of Illinois at Urbana-Champaign

Federated Authentication

- The provider of the identity and the provider of the service (uPortal) may not be the same institution
- Users can authenticate using identities from anywhere in federation, to services anywhere in federation, with a healthy policy layer.

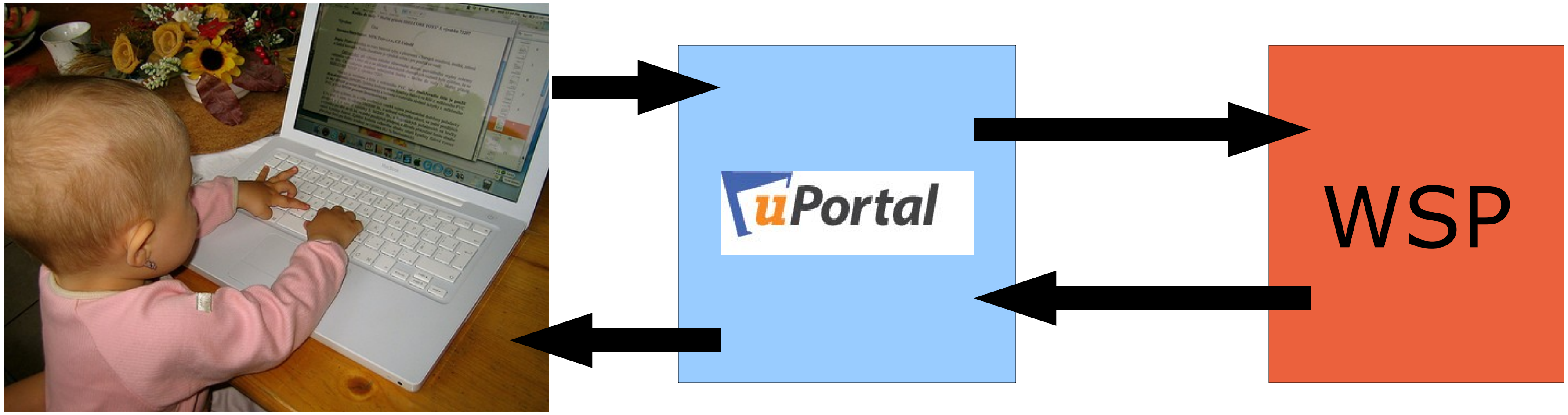
InCommon®

Attribute release

- Just in time release of attributes to the portal at the time of user authentication
- Different from querying directories of attributes
  - Attributes released only in context of actual user authentication
  - Attributes may be of a federated identity, attribute information not necessarily available to portal in an institutional directory

Delegated authentication

- User authenticates to portal
- Portal authenticates to a backing service on behalf of the user
- Data from backing service informs portal



http://www.flickr.com/photos/ntr23/730371240/

Shibbolizing uPortal Today

Authentication
Attribute Release

Authenticating to uPortal with Shibboleth

Authentication

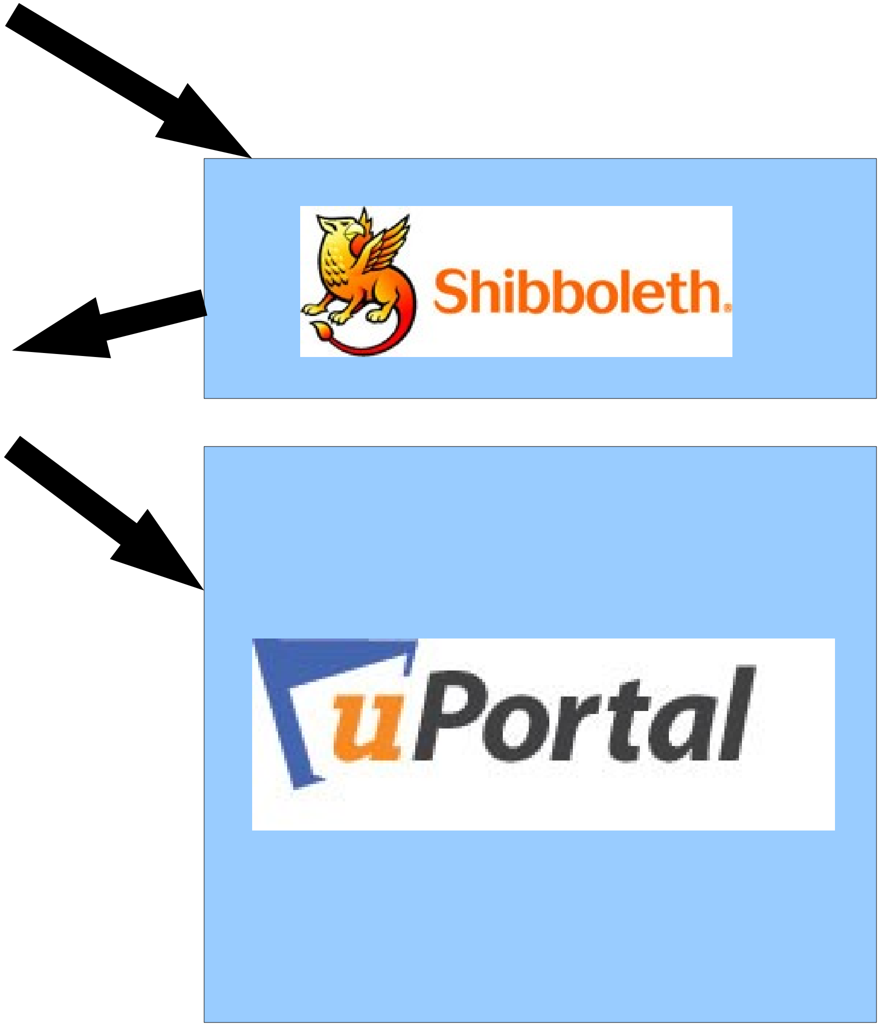
Shibboleth for Authentication

- Shibboleth provides a Service Provider Apache module for authentication
- uPortal can delegate to container for authentication
- Ta-da!

Shibboleth SP Authentication

<Assertion/>

HTTP: headers



HTTP Headers

HTTP headers set by the Shibboleth SP represent the authenticated user identifier (remote user) and user attributes

Shibbolizing CAS?

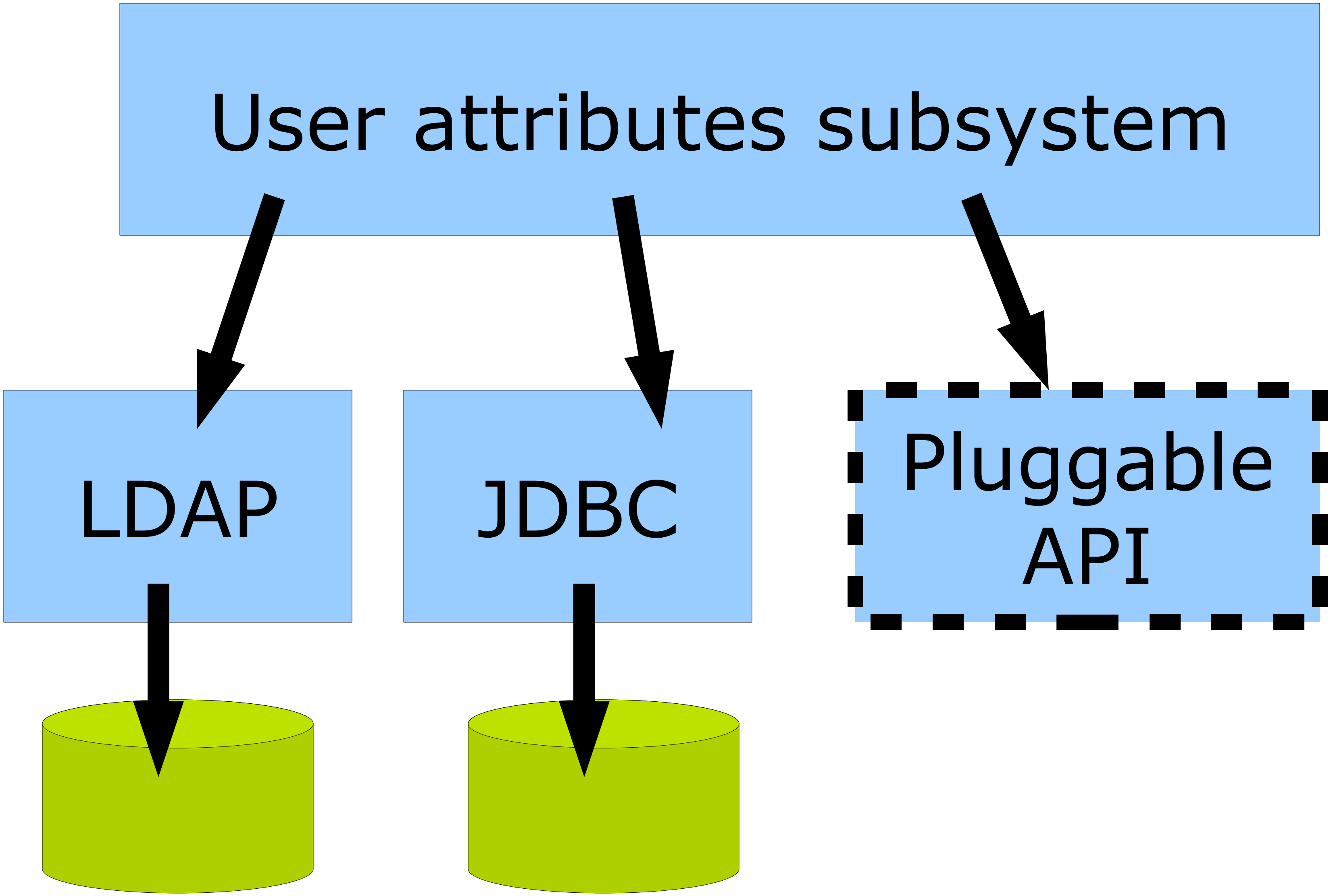
- uPortal ships with a CAS server and support for using CAS for login
- CAS can be easily Shibbolized
- Shibbolize uPortal by Shibbolizing CAS?

http://www.flickr.com/photos/javaturtle/117152990/

Releasing Attributes to uPortal with Shibboleth

Attributes

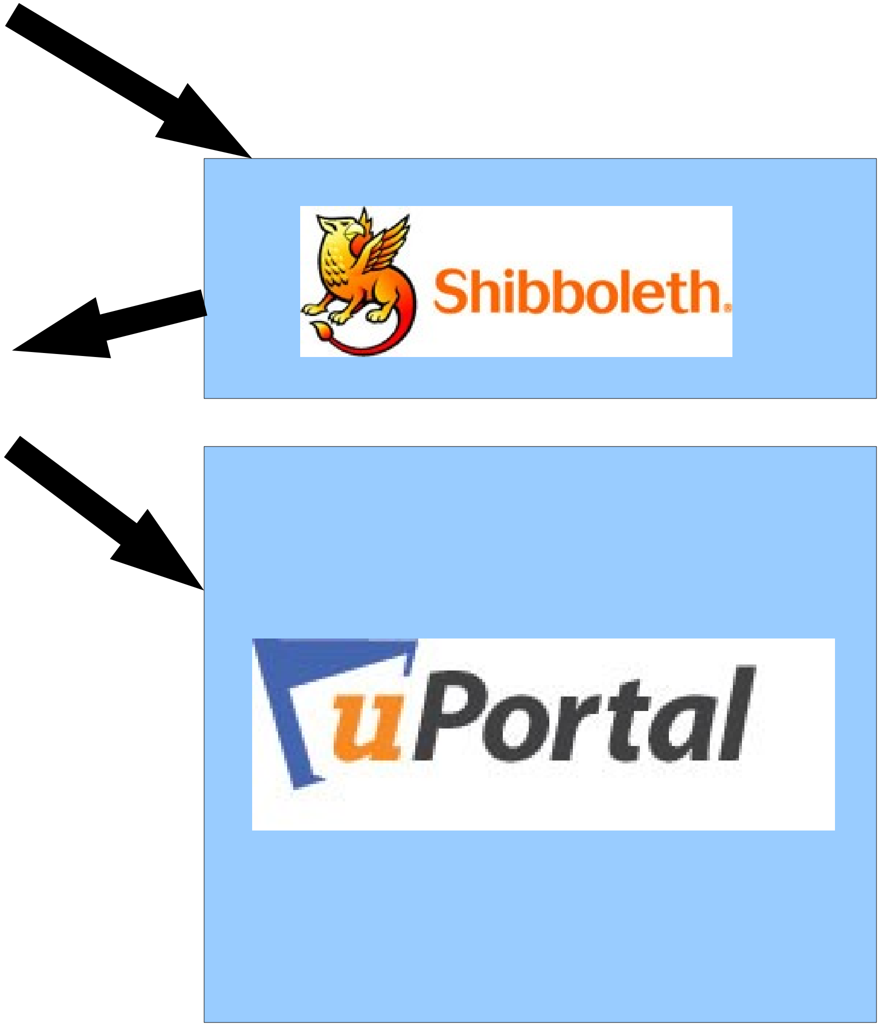
User Attributes in uPortal



Shibboleth attribute release

<Assertion/>

HTTP: headers

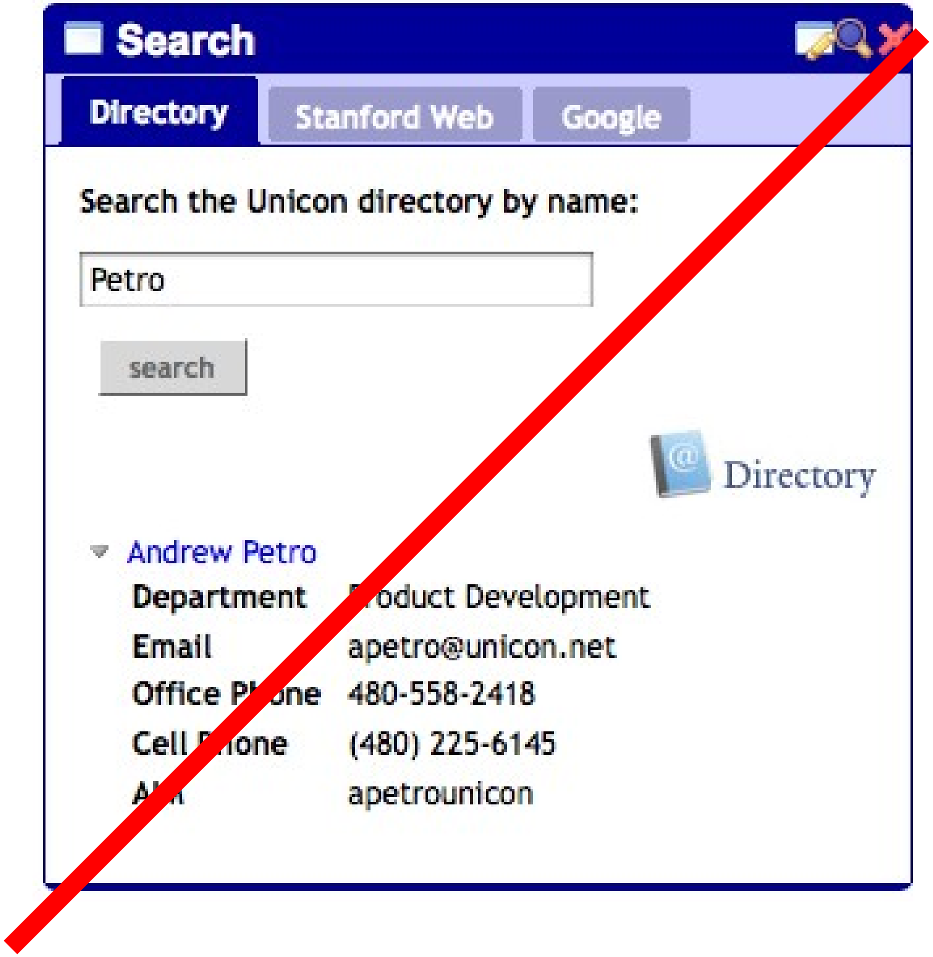


HTTP Headers

HTTP headers set by the Shibboleth SP represent the authenticated user identifier (remote user) and user attributes

User attributes at login

- User attributes in the context of user login
- Not arbitrary queries of directories



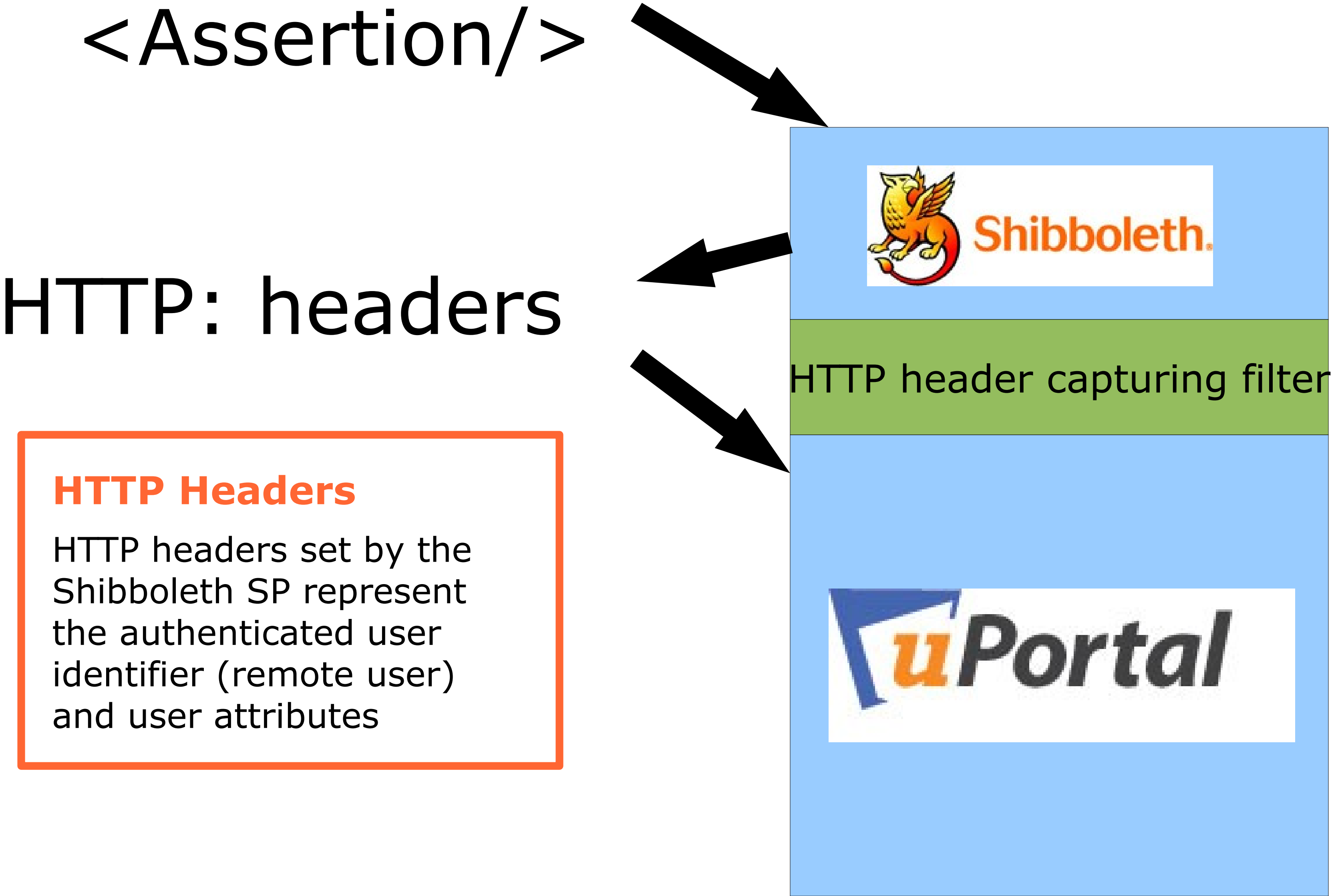
Search the Unicon directory by name:

Petro

Andrew Petro

Department	Product Development
Email	apetro@unicon.net
Office Phone	480-558-2418
Cell Phone	(480) 225-6145
AIM	apetrounicon

Capturing user attributes from SP



<Assertion/>

HTTP: headers

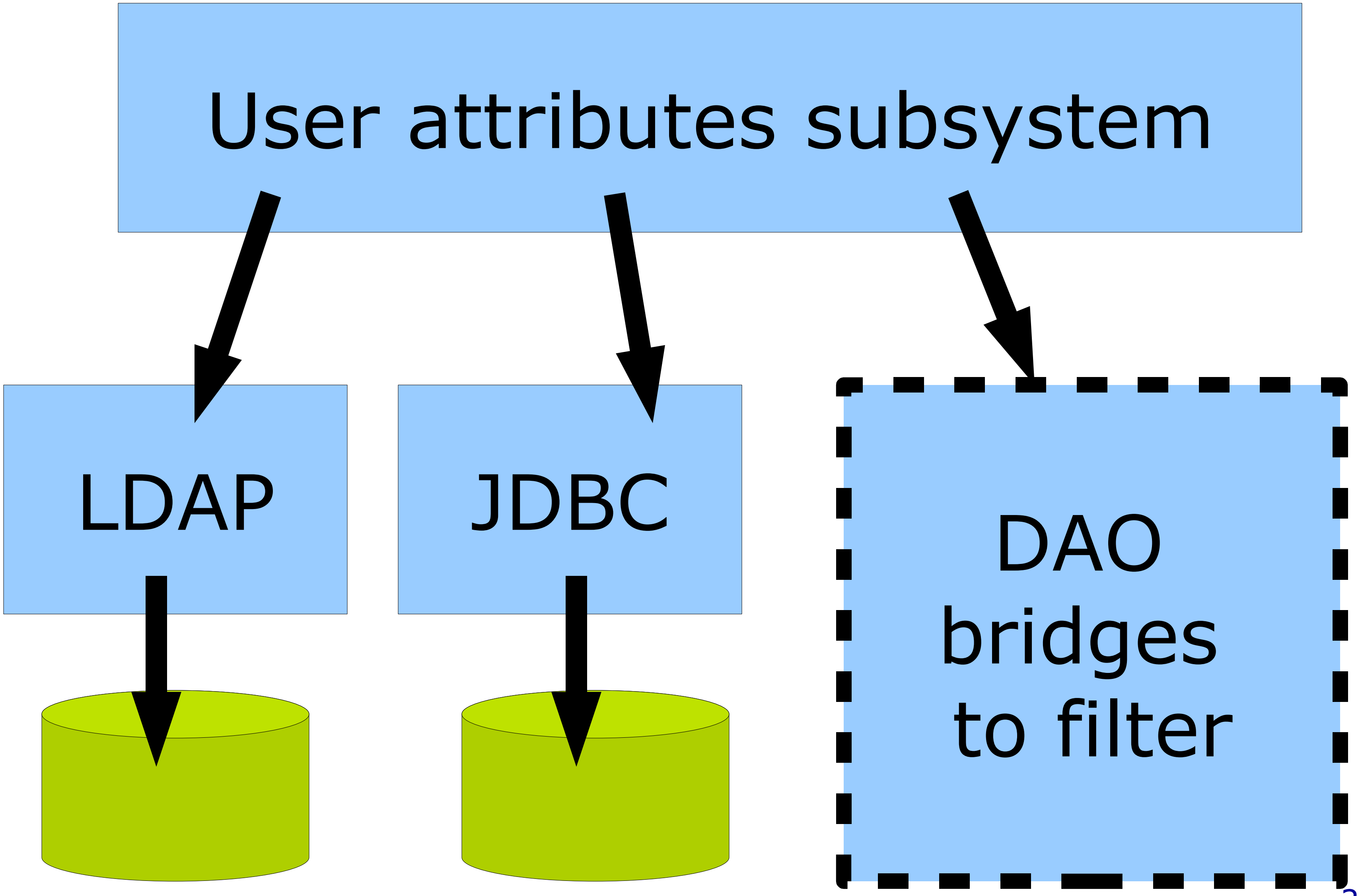
HTTP Headers

HTTP headers set by the Shibboleth SP represent the authenticated user identifier (remote user) and user attributes

Declare the filter in web.xml

```xml
<filter>
  <filter-name>HttpHeaderFilter</filter-name>
  <filter-class>edu.jhu.services.persondir.support.http.HttpHeaderFilter</filter-class>
  <init-param>
    <param-name>personDirectoryDaoName</param-name>
    <param-value>httpHeaderAttributeSource</param-value>
  </init-param>
</filter>
<filter-mapping>
    <filter-name>HttpHeaderFilter</filter-name>
    <servlet-name>Login</servlet-name>
</filter-mapping>
```

User attributes from Shibboleth



Declare the attribute source

```
<list>
  <ref bean="uPortalJdbcAttributeSource"/>
  <ref bean="uPortalLdapAttributeSource"/>
  <ref bean="httpHeaderAttributeSource"/>
</list>
```

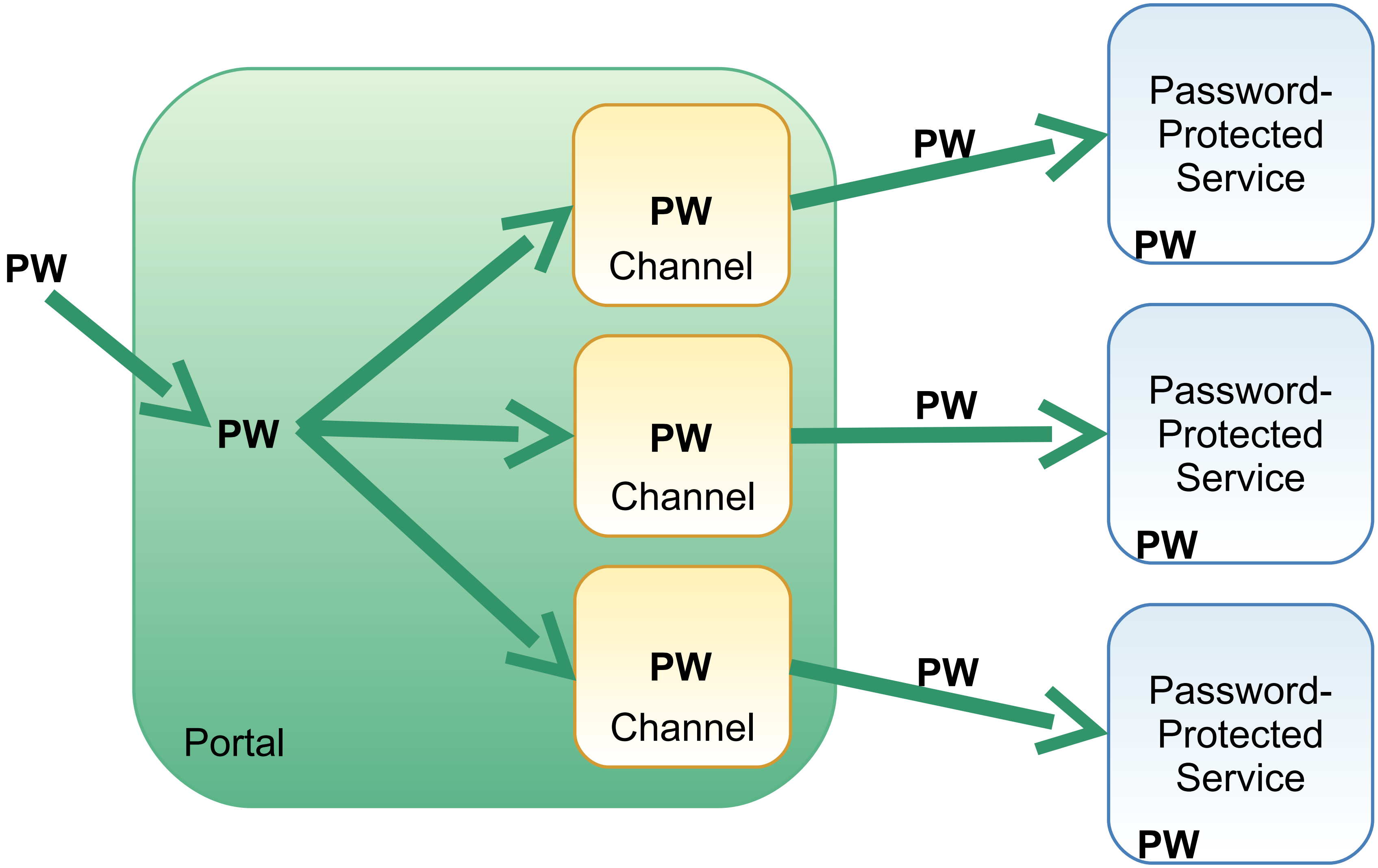
Canonical way to do this is in flux

- Not very much in flux, but a little in flux
- In Jira: PERSONDIR-37, PERSONDIR-49
- The (a) DAO for this ships in Persondir 1.5 RC2
- For now, if you're interested, please ping me.
- apetro@unicon.net

Delegated Shibbolized Authentication...

In uPortal

Password Replay

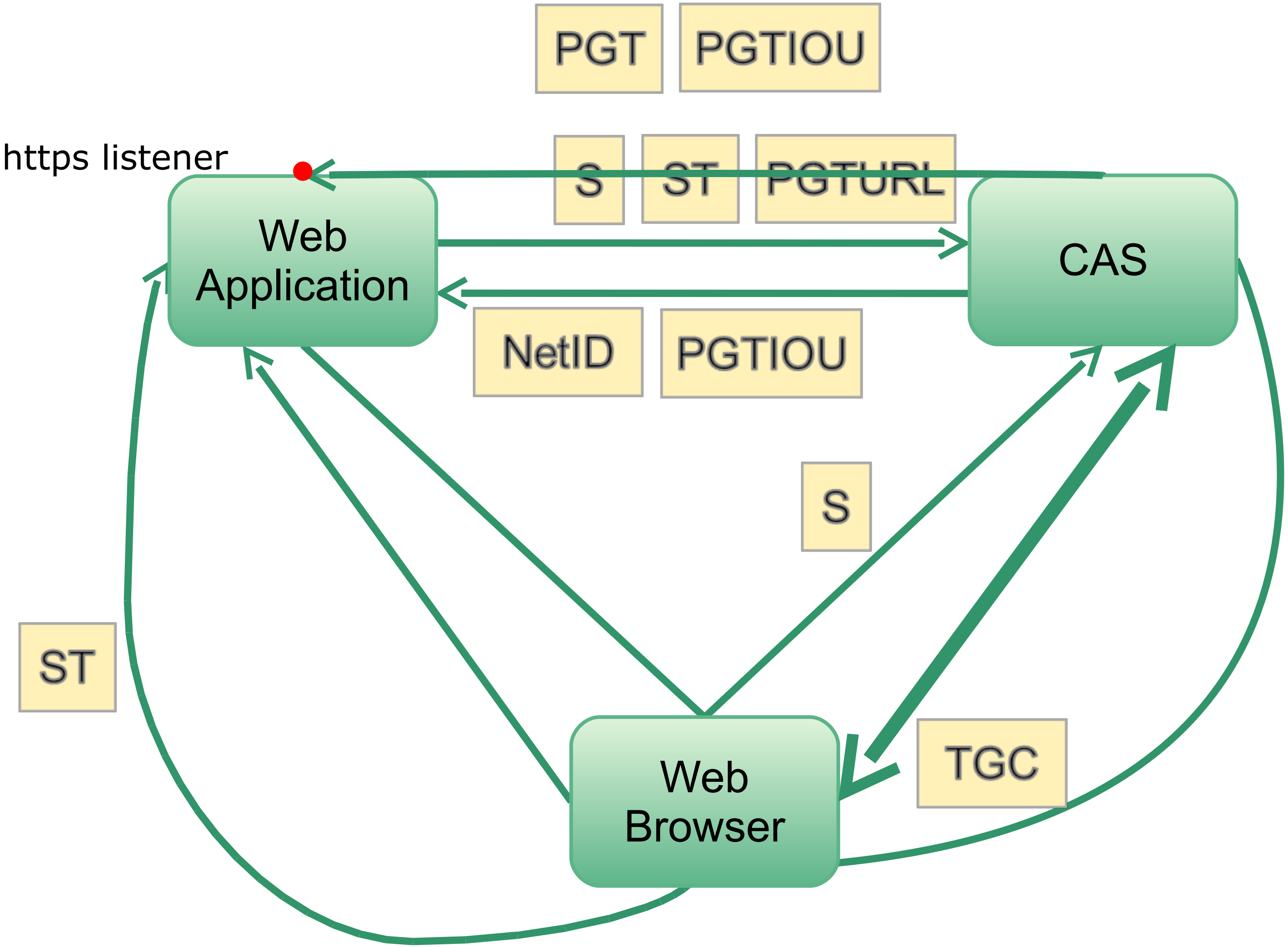

PW
PW
Portal
PW
Channel
PW
Channel
PW
Channel
PW
PW
PW
Password-Protected Service
PW
Password-Protected Service
PW
Password-Protected Service
PW

Look Ma, No Password!

- Without a password to replay, how am I going to authenticate my portal to other applications?

?

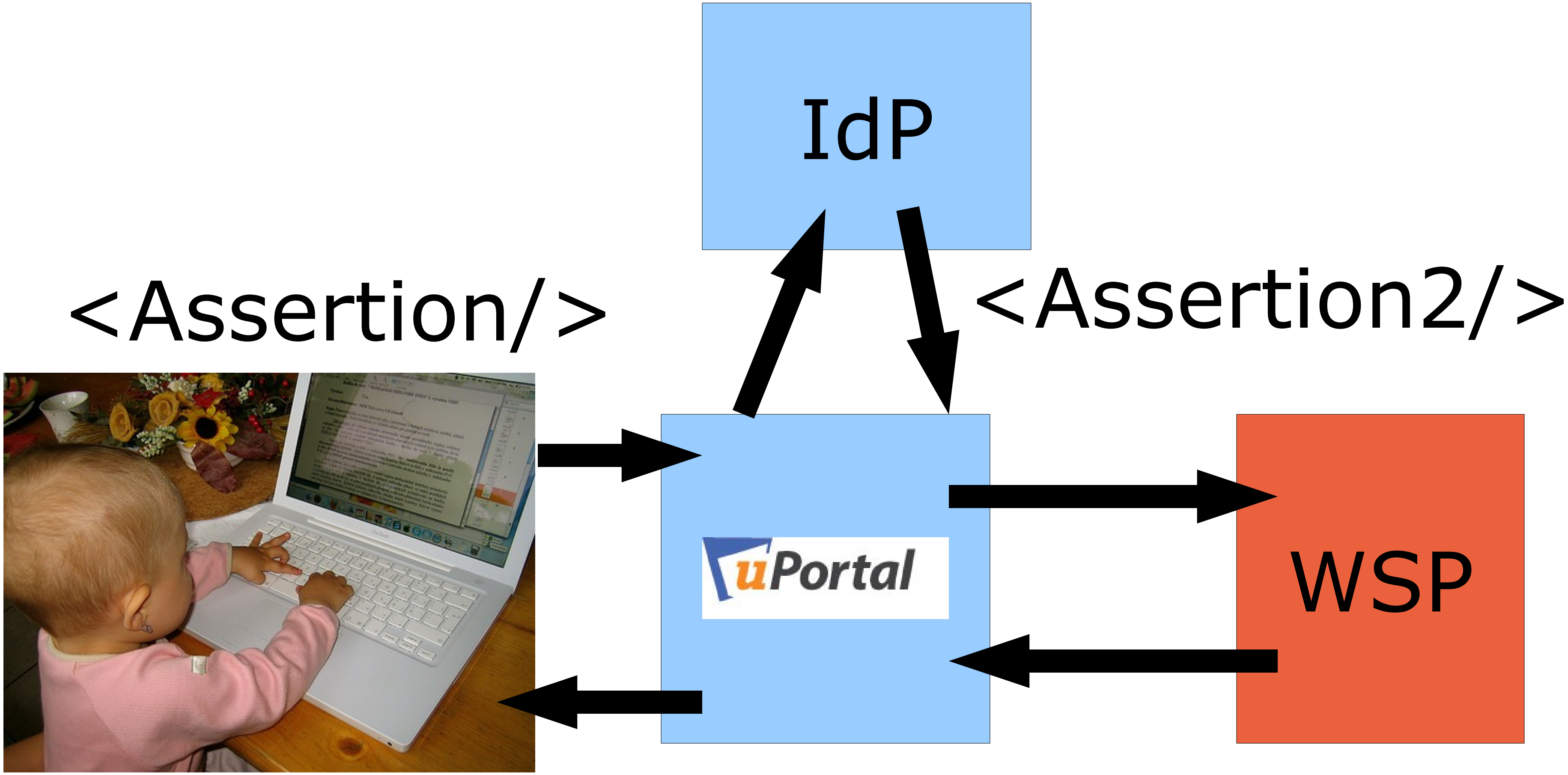
Proxy CAS


PGT
PGTIOU
https listener
S
ST
PGTURL
Web Application
CAS
NetID
PGTIOU
S
ST
TGC
Web Browser

Oh, wait, this is Shibboleth

- Very similar idea.
- Portal presents SAML Assertion to Portlet
- Portlet presents SAML Assertion to IdP
- IdP issues Portlet a new SAML Assertion for purpose of authenticating Portlet to backing Web Service Provider
- Portlet presents Assertion to backing Web Service Provider, authenticating its request to the backing service.

Delegated authentication



IdP

<Assertion/>

<Assertion2/>

uPortal

WSP

Getting the SAML to the Portlet

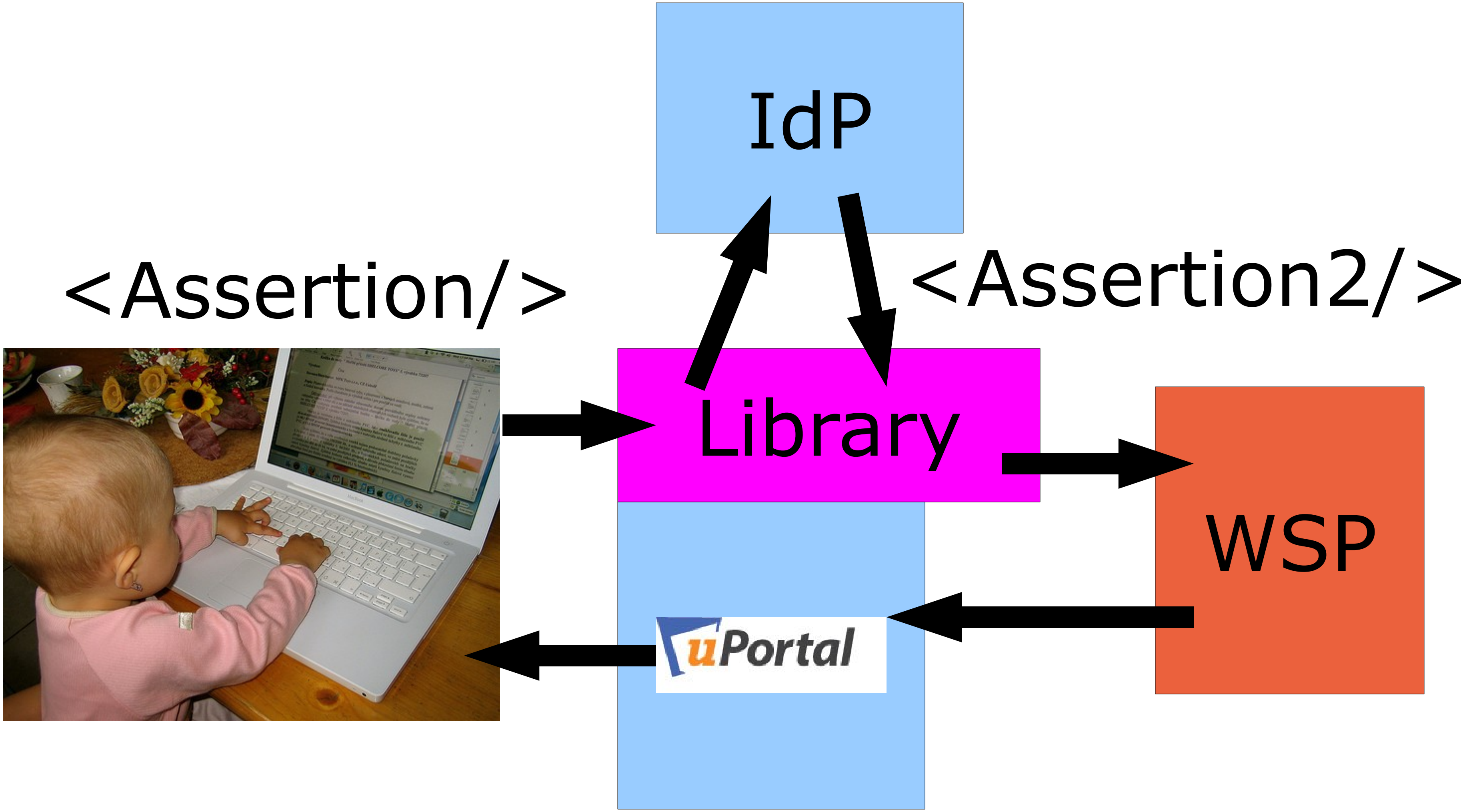
- Solution parallel to that for conveying passwords and CAS Proxy Tickets to portlets
- Custom UserInfoService
- Portlets obtain SAML assertions (like passwords and CAS proxy tickets) via callback for a “magic” user attribute

SAML to authenticate to a WSP

- Portlet presents SAML to IdP to get more SAML to present to backing WSP

- Wouldn't it be nice if there were a library that automated this?
  - Abstract away the (re-)authentication part
  - Present to portlet either simple response from WSP or an API to make further requests
  - Think adorned Commons HttpClient

Delegated authentication



IdP

<Assertion/>

<Assertion2/>

Library

WSP

uPortal

Delegated Shibbolized Authentication…

In Shibboleth

Defer to the other slide deck...

- One moment please...

Concluding remarks

Where to learn more

- Internet2 Wiki Space:
- https://spaces.internet2.edu/x/TTM
- Tom Barton, Scott Cantor, Andrew Petro, Adam Rybicki, and Tamra Valadez at this conference

Questions & Answers