

שבולת

SD Departmental Meeting
November 28th, 2006

Ale de Vries
Product Manager ScienceDirect
Elsevier

Shi... whát?

שבולת : Shibboleth

[...] "stream, torrent". It derives from a story in the Hebrew Bible, in which pronunciation of this word was used to distinguish members of a group (like the Ephraimites) whose dialect lacked a /ʃ/ sound (as in shoe) from members of a group (like the Gileadites) whose dialect did include such a sound.

[<http://en.wikipedia.org/wiki/Shibboleth>]

Some concepts
Elsevier's view
About Shibboleth
Then
Now
Later
Questions

Some concepts

AuthN: authentication

who are you

AuthZ: authorization

what are you allowed to

Authentication methods

Traditional authentication technologies

- IP address checking
- Username/password

Shared authentication technologies

- Centralized Authentication
- Federated or Distributed Authentication

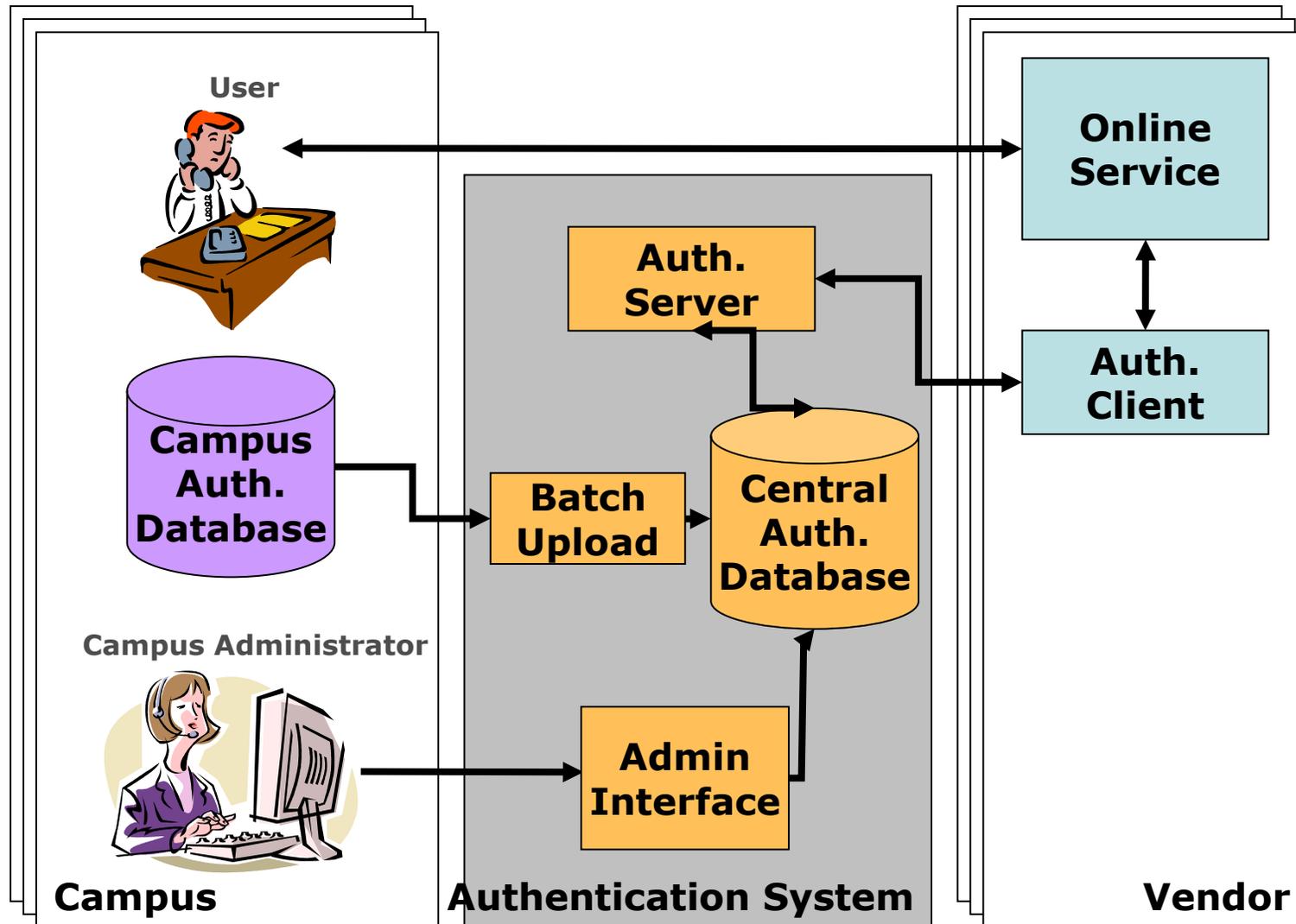
IP Address Checking

Pros	<ul style="list-style-type: none">• Supports site-wide access• Supports anonymous access• Supports walk-ins
Cons	<ul style="list-style-type: none">• Maintenance overhead for customer and vendor• Inherently insecure• Dependency on network topology• No native support for remote access

Username/Password

Pros	<ul style="list-style-type: none">• Supports remote access• Allows personalization
Cons	<ul style="list-style-type: none">• Need a different username for every service• Complex administration for remote access<ul style="list-style-type: none">– No standard between vendors• “Leaky”:<ul style="list-style-type: none">– Password sharing– No easy way to de-activate users when they leave the authorised community

Centralised Authentication

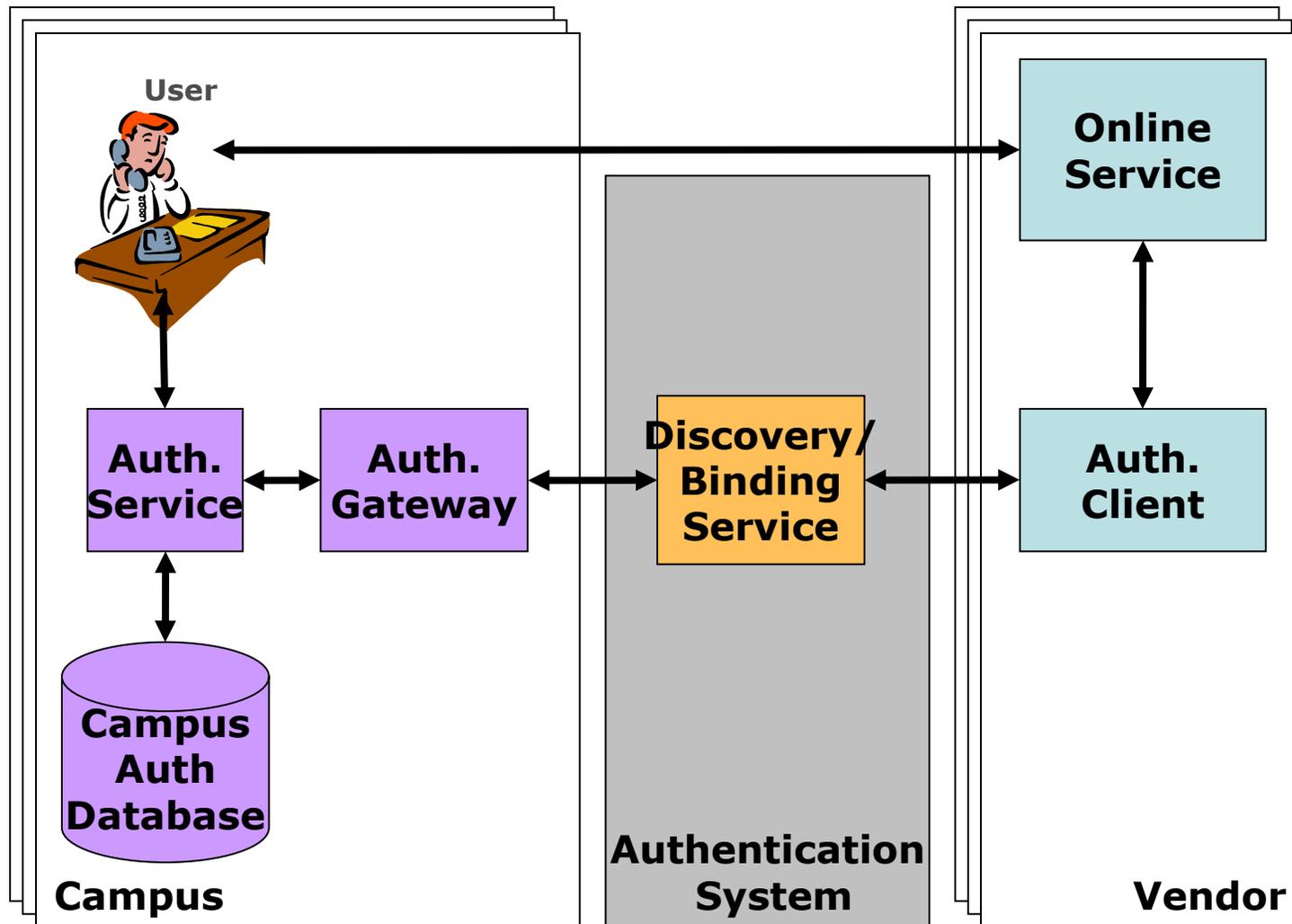


Centralised Authentication – cont’d

Pros	<ul style="list-style-type: none">• Single un/pw for multiple services• Remote access• Little or no IT implementation for customer
Cons	<ul style="list-style-type: none">• Administrative overhead for customer• Need for synchronisation between campus and central authentication database• Use different user credentials for central service logon vs. campus logon• Batch, not real-time (aging technology)

Example: “Classic” Athens (UK)

Federated Authentication



Federated Authentication – cont'd

Pros	<ul style="list-style-type: none">• Allows access to remote services using campus logon credentials• No extra administrative overhead for customer• Simpler for users
Cons	<ul style="list-style-type: none">• More complex technical implementation for institution• Requires agreement on “rules of the game” between all vendors and institutions.

Example: Shibboleth, Athens DA

Our imperative



No matter what, we will always provide...:

- anonymous blanket access
- optional personalized services in exchange of basic registration

... using whatever methods are common practice with our customers

We **like** federated authentication 😊

- Replacement for IP authentication for on-site access
- Remote access! and personalization using local credentials (no more post-its)

Fulfils customer needs

Makes our lifes easier

(It's what the world is moving to)

Shibboleth is many things...

- **A protocol specification**
- **An architecture**
- **Some open-source software** which implements the architecture
- **A project** which manages definition of the protocol, architecture and development of the software
- Developed by MACE of the Internet2 Consortium in the USA, using standards like SAML and PKI

... but what does it do?

It allows **users** to get access to online resources with their organization's un/pw

(... while providing the involved parties with a framework for the underlying technical, operational, organizational, legal etc. aspects)

Shib & SD history: ramp-up...



- April 2002: Attended DLF/CNI workshop at NYU
- Held workshops to involve customers and Internet 2 in design. Findings:
 - Anonymous non-personalized access a must
 - Provide option to personalize if an opaque, unique user identifier is supplied
 - Needed support for deep linking
- May 2004: Initial Shib release
 - Support for a single Federation... initially InQueue

Shib & SD history: ... testing...



- May-Dec 2004: Pilot test
- Participants: Dartmouth; Georgetown; NYU; UCSD; Penn State
- Pilot aims:
 - What does it take to get campuses up and running?
 - What end-user issues arise?
- No major problems getting up and running
 - Some issues with attributes, release policies, firewalls
- None of the pilot participants rolled out access to broad user community

Shib & SD history: ... production!



- Feb 2005: Moved in InCommon (US Production Federation)
 - First vendor to use InCommon in production
- July 2005: Multi-federation support released
 - Challenge: how to deal with a multi-federation world
 - Held more design workshops with representatives from multiple federations around the world

Role of Shibboleth Federations



- Act as naming authority for members
- Manage operational metadata about members
- Establish trust framework
 - in practice by acting as Certificate Authority for SAML and SSL signing certificates
- Set common policies for members
- Vet members
- Provide infrastructure for identity provider discovery (Where Are You From - WAYF)
- Define vocabularies of attributes and semantics

Multiple federations



SDSS



SWITCH



InCommon®

haka



The WAYF issue

- WAYF (Where Are You From) page: from what institution are you?
 - Normally operated by federation
 - Multi-federation support means: from what federation are you?
 - No-one runs a WAYF of WAYFs
- ☹ End users don't understand the federation concept
- ☺ ... but federations are geographically oriented!
- Our solution: implement WAYF inside ScienceDirect
 - Label federations geographically

The example scenario...



- Logging in to ScienceDirect with a local University of Tilburg username and password
- Live in production!

ScienceDirect - Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://www.sciencedirect.com/science> Go Links

msn Search Web Form Fill Blocked (29) My MSN

ScienceDirect - Home

 **SCIENCE @ DIRECT**

Register or Login: user name Password: Go **Athens/Institution Login**

Home Search Journals Books Abstract Databases My Profile Alerts Help

Quick Search: within All Full-text Sources Go Search Tips

Full-text articles in ScienceDirect: 7,178,672

ScienceDirect Info

- [About ScienceDirect](#)
- [Content Coverage](#)
- [Librarian Services](#)
- [Guest User Info](#)
- [About Athens](#)
- [Why Register?](#)
- [User Guides](#)
- [ScienceDirect News](#)
- [Contact Us](#)
- [More Info...](#)

ScienceDirect®

Welcome to the world's largest electronic collection of science, technology and medicine full text and bibliographic information.

Introducing ScienceDirect **College Edition**. Specifically designed to meet their needs, ScienceDirect is now available for colleges in North and South America.

Over 1800 titles online...

Search for a Title: go

OR **Browse A-Z**

Top Publications in ScienceDirect

-  FEMS Microbiology Reviews
-  Progress in Materials Science
-  Applied and Computational Harmonic Analysis

Hot Topics

- Accountants Are Boring Because Of The

Subject Areas in ScienceDirect

- [Agricultural and Biological Sciences](#)
- [Arts and Humanities](#)
- [Biochemistry, Genetics and Molecular Biology](#)
- [Business, Management and Accounting](#)
- [Chemical Engineering](#)
- [Chemistry](#)
- [Computer Science](#)
- [Decision Sciences](#)
- [Earth and Planetary Sciences](#)
- [Economics, Econometrics and Finance](#)
- [Energy](#)
- [Engineering](#)
- [Environmental Science](#)
- [Immunology and Microbiology](#)
- [Materials Science](#)
- [Mathematics](#)
- [Medicine and Dentistry](#)

Internet

ScienceDirect - Login via Athens or Your Institution - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail New Tab

Address http://www.sciencedirect.com/science?_ob=FederationURL&_method=display&_type=f&_acct=C000000593&_version=1&_userid=3222073&md5=6b9b79b46e0b45e Go Links

msn Search Web Form Fill Blocked (29) Spaces My MSN

ScienceDirect - Logi...



Register or Login: Password: Go [Athens/Institution Login](#)

Home Search Journals Books Abstract Databases My Profile Alerts Help

Quick Search: within Go [Search Tips](#)

Login via Athens or Your Institution

You may be able to login to ScienceDirect using Athens or your institution's login credentials. We will 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.

Go

[View All Institutions](#)

Home Search Journals Books Abstract Databases My Profile Alerts Help

[Contact Us](#) | [Terms & Conditions](#) | [Privacy Policy](#)

Copyright © 2005 [Elsevier B.V.](#) All rights reserved. ScienceDirect® is a registered trademark of Elsevier B.V.

Done Internet

ScienceDirect - Login via Athens or Your Institution - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail New Tab

Address http://www.sciencedirect.com/science/page/static/science/science?_ob=FederationURL&_method=display&md5=e2d806d1e8c4953bc9f57621cb18fbd2&fedId=4 Go

msn Search Web Form Fill (5) Spaces My MSN News

ScienceDirect - Logi...

 **SCIENCE @ DIRECT**

Register or Login: Password: [Athens/Institution Login](#)

[Home](#) [Search](#) [Journals](#) [Books](#) [Abstract Databases](#) [My Profile](#) [Alerts](#) [Help](#)

Quick Search: within [Search Tips](#) Brought to you by: [The ScienceDirect Team](#)

Login via Athens or Your Institution

You may be able to login to ScienceDirect using Athens or your institution's login credentials. We will 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.

[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.

Dutch Universities

- [SURFnet Identity Provider](#)

[Home](#) [Search](#) [Journals](#) [Books](#) [Abstract Databases](#) [My Profile](#) [Alerts](#) [Help](#)

[Contact Us](#) | [Terms & Conditions](#) | [Privacy Policy](#)

Copyright © 2006 [Elsevier B.V.](#) All rights reserved. ScienceDirect® is a registered trademark of Elsevier B.V.

Help is Available Internet



Shibboleth Handle Request Processed - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Links Hotmail NonSolus

Address <https://rivest.surfnet.nl/shibboleth/H5?target=https%3A%2F%2Fsdauth.sciencedirect.com&shire=https%3A%2F%2Fsdauth.sciencedirect.com%2F5HIRE&providerId=https%3A%2F%2Fsdauth.sciencedirect.com%2F5HIRE> Go

msn Search Web Form Fill (5) Spaces My MSN News

Shibboleth Handle Re...

Shibboleth Handle 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...

Opening page <https://sdauth.sciencedirect.com/SHIRE...> Internet

ScienceDirect - Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail New Tab

Address http://www.sciencedirect.com/science Go

msn Search Web Form Fill (5) Spaces My MSN News

ScienceDirect - Home

 **SCIENCE @ DIRECT**

Home Search Journals Books Abstract Databases My Profile Alerts Help

Quick Search: within All Full-text Sources [Search Tips](#)

Brought to you by: Tilburg University

Full-text articles in ScienceDirect: 7,972,303

ScienceDirect Info

- [About ScienceDirect](#)
- [Content Coverage](#)
- [Librarian Services](#)
- [Guest User Info](#)
- [About Athens](#)
- [Why Register?](#)
- [User Guides](#)
- [ScienceDirect News](#)
- [Contact Us](#)
- [More Info...](#)

ScienceDirect®

Welcome to the world's largest electronic collection of science, technology and medicine full text and bibliographic information.

Elsevier Admin Tool The best way to manage your ScienceDirect account. [Learn more...](#)

Over 1800 titles online...

Search for a Title:

OR [Browse A-Z](#)

Top Publications in ScienceDirect

-  [Current Opinion in Plant Biology](#)
-  [Biochimica et Biophysica Acta - Reviews on Cancer](#)
-  [Journal of Accounting and Economics](#)

Hot Topics

- Mum's baby blues slows kids' language and...

Subject Areas in ScienceDirect

- ▶ [Agricultural and Biological Sciences](#)
- ▶ [Arts and Humanities](#)
- ▶ [Biochemistry, Genetics and Molecular Biology](#)
- ▶ [Business, Management and Accounting](#)
- ▶ [Chemical Engineering](#)
- ▶ [Chemistry](#)
- ▶ [Computer Science](#)
- ▶ [Decision Sciences](#)
- ▶ [Earth and Planetary Sciences](#)
- ▶ [Economics, Econometrics and Finance](#)
- ▶ [Energy](#)
- ▶ [Engineering](#)
- ▶ [Environmental Science](#)
- ▶ [Immunology and Microbiology](#)
- ▶ [Materials Science](#)
- ▶ [Mathematics](#)
- ▶ [Medicine and Dentistry](#)

Logged in via SURFnet Identity Provider [Logout](#)

Internet

ScienceDirect - Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail New Tab

Address http://www.sciencedirect.com/science Go

msn Search Web Form Fill (5) Spaces My MSN News

ScienceDirect - Home

 **SCIENCE @ DIRECT**

Register or Login: Password: [SURFnet Identity Provider Login](#) [Athens/Other Institution Login](#)

Home Search Journals Books Abstract Databases My Profile Alerts  Help

Quick Search: within  Search Tips

Brought to you by: [The ScienceDirect Team](#)

Full-text articles in ScienceDirect: **7,372,303**

ScienceDirect Info

- [About ScienceDirect](#)
- [Content Coverage](#)
- [Librarian Services](#)
- [Guest User Info](#)
- [About Athens](#)
- [Why Register?](#)
- [User Guides](#)
- [ScienceDirect News](#)
- [Contact Us](#)
- [More Info...](#)

ScienceDirect®

Welcome to the world's largest electronic collection of science, technology and medicine full text and bibliographic information.

Elsevier Admin Tool The best way to manage your ScienceDirect account. [Learn more...](#)

Over 1800 titles online...

Search for a Title:

OR [Browse A-Z](#)

Top Publications in ScienceDirect

 Current Opinion in Plant Biology	 Biochimica et Biophysica Acta - Reviews on Cancer	 Journal of Accounting and Economics
---	--	--

Hot Topics

- Mum's baby blues slows kids' language and...

Subject Areas in ScienceDirect

- ▶ [Agricultural and Biological Sciences](#)
- ▶ [Arts and Humanities](#)
- ▶ [Biochemistry, Genetics and Molecular Biology](#)
- ▶ [Business, Management and Accounting](#)
- ▶ [Chemical Engineering](#)
- ▶ [Chemistry](#)
- ▶ [Computer Science](#)
- ▶ [Decision Sciences](#)
- ▶ [Earth and Planetary Sciences](#)
- ▶ [Economics, Econometrics and Finance](#)
- ▶ [Energy](#)
- ▶ [Engineering](#)
- ▶ [Environmental Science](#)
- ▶ [Immunology and Microbiology](#)
- ▶ [Materials Science](#)
- ▶ [Mathematics](#)
- ▶ [Medicine and Dentistry](#)

SD @ Connect Product News Letter SUBSCRIBE NOW! ▶▶

Internet

Driving Adoption - Federations



- Standardisation across federations is needed to ease Service Provider implementation, especially
 - Attribute syntax and semantics (good progress recently!)
 - Certificates
 - Metadata distribution policy
 - IdP granularity
- Advice: do what's been done before, don't reinvent the wheel

Driving Adoption – Service Providers

- Act now!
 - Your customers will be asking you for this if they haven't already
- Get involved in the community – shibboleth-users listserv (shibboleth-users@internet2.edu)
- Understand the concepts and architecture
- Use the standard open-source implementation

Driving Adoption - Institutions



- Decide who owns Shibboleth
 - Central IT?
 - Library?
 - Administration?
- Largest barrier: central source of identity for all users
 - Central Admin/HR database?
 - Library patron database?
 - Computing centre/IT user database?
- Shib software integration is relatively easy
- Need a killer-app to drive take-up

Open Issues and the Future...



- Technology new, complex and rapidly changing
- Federations are in very early stages
- Uptake is key... we are in a critical phase
- Need to make implementation easier for smaller customers and vendors
- Elsevier is committed to making access easier for users and will continue to support Shibboleth

שאלה?

more info: ale@elsevier.com

End of presentation...



Shibboleth Mechanics

So what's going on here?



The Shibboleth framework allows

Identity Providers (IdPs)

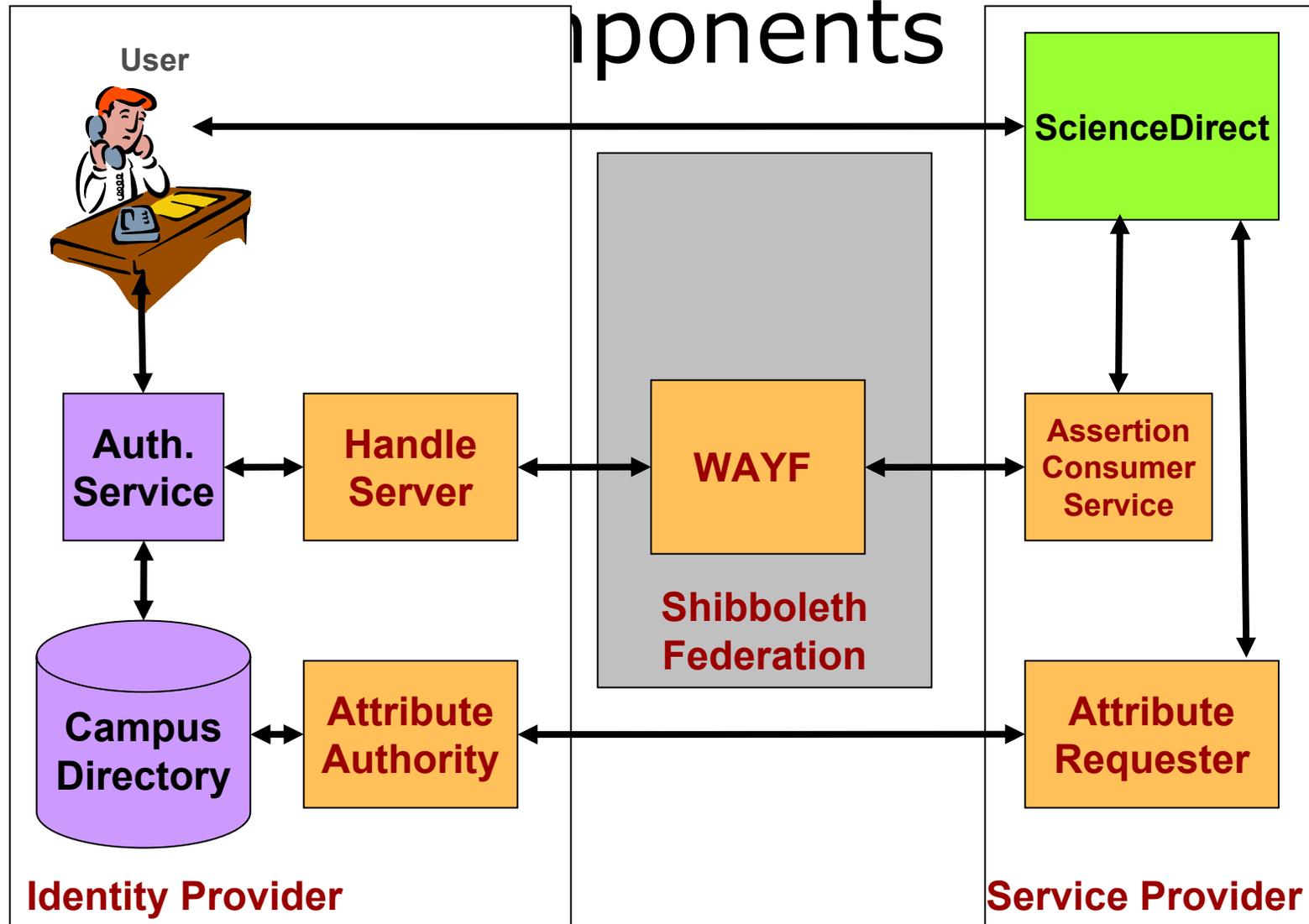
to make

Trusted Assertions

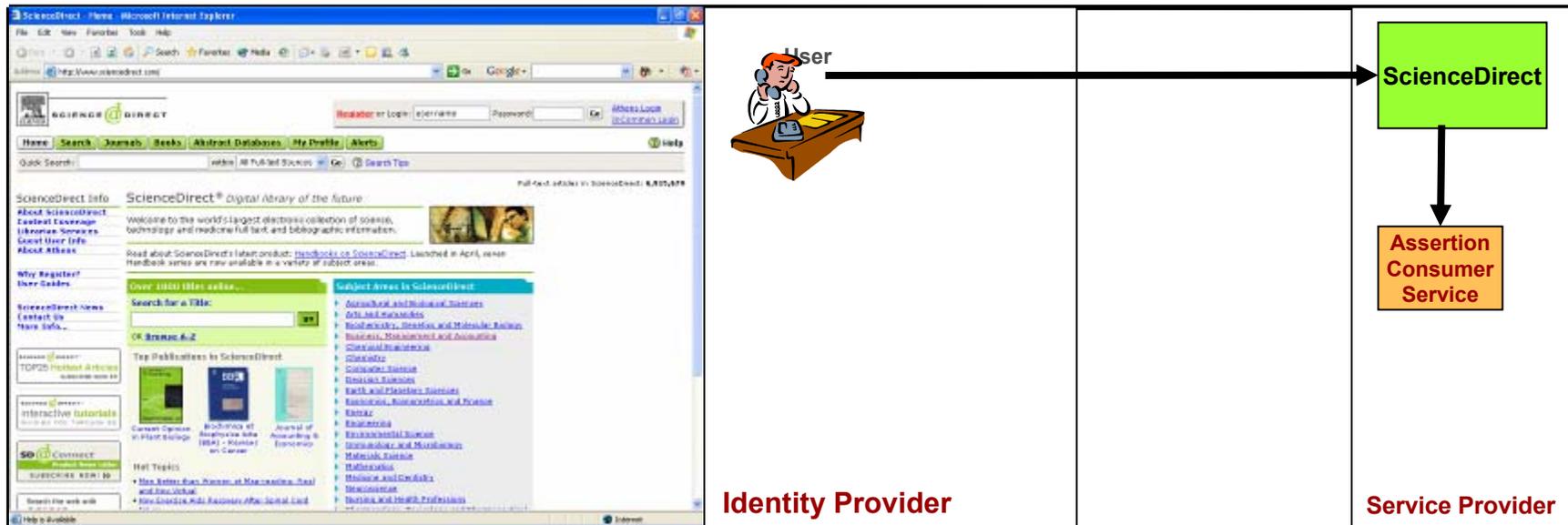
about users to

Service Providers (SPs)

Shibboleth Software

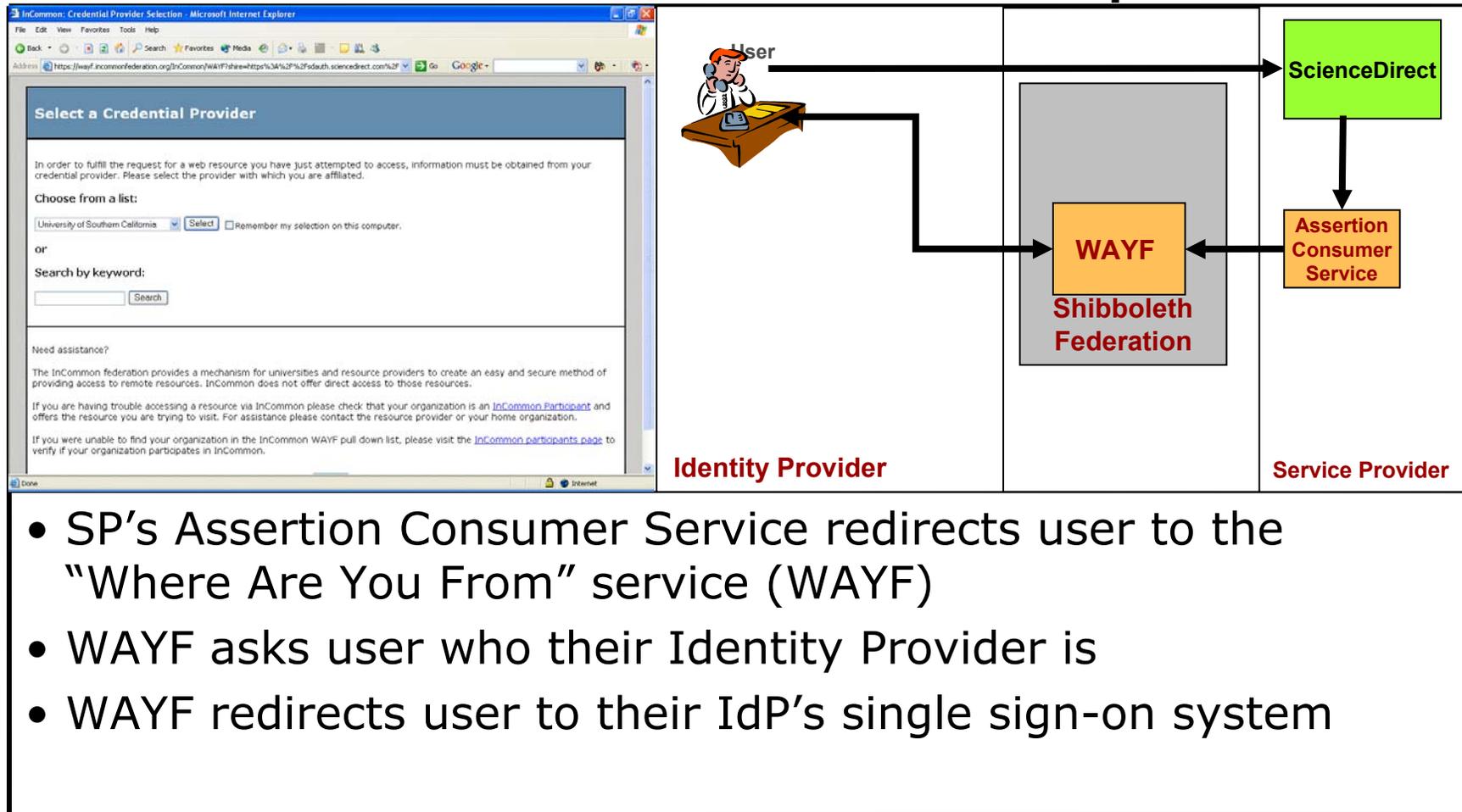


Shibboleth Flow - Step 1

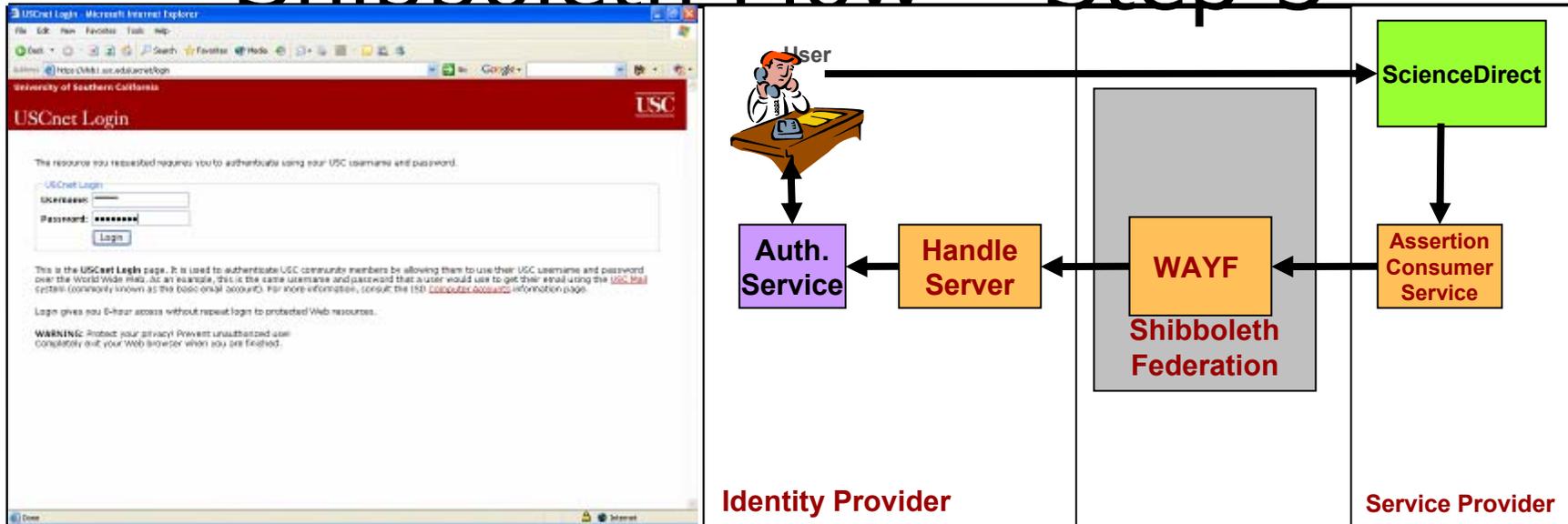


- User goes to protected resource, e.g. www.sciencedirect.com
- User requests to be authenticated by Shibboleth
- Resource passes control to SP's Assertion Consumer Service

Shibboleth Flow – Step 2

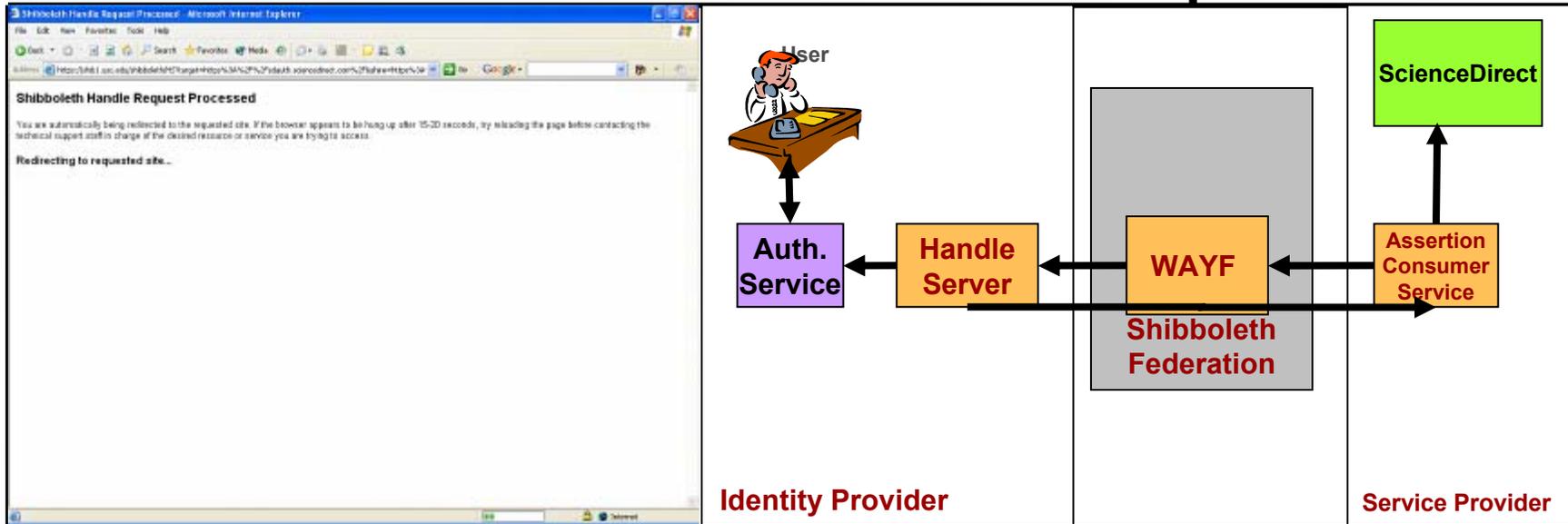


Shibboleth Flow – Step 3



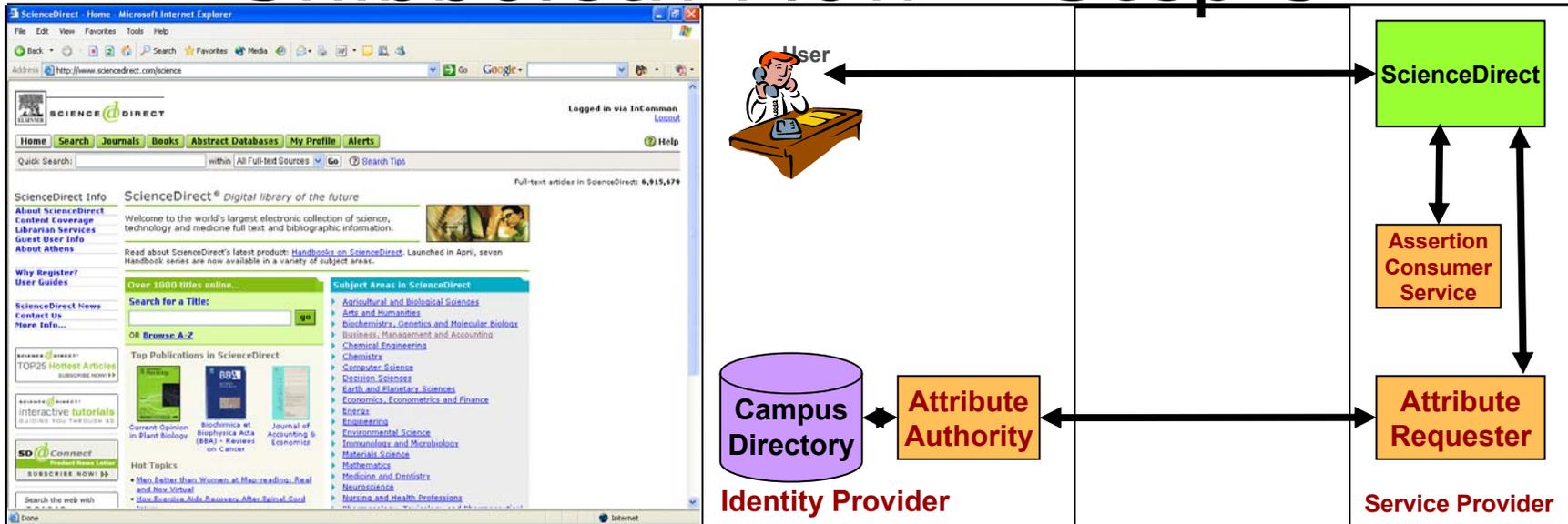
- User logs in to their IdP's single sign-on system
- IdP's single sign-on system authenticates user

Shibboleth Flow – Step 4



- IdP's single sign-on system redirects user to SP's Assertion Consumer Service providing unique handle for session

Shibboleth Flow – Step 5



- SP's Attribute Requester uses handle to request needed information about the user from the IP's Attribute Authority
- IdP's Attribute Authority retrieves requested attributes about user from campus directory and transmits securely to SP
- Upon receiving appropriate attributes, SP authorizes user's request to access resource

How is trust established?

- Assertions are signed using PKI certificates according to SAML standard (Security Assertion Markup Language)
- Interactions are SSL encrypted
- Trust is facilitated by “Federations”
 - Groups of organizations that agree to deploy Shibboleth according to certain operating principles, sharing common metadata and attribute definitions, etc.

Attribute Exchange

- Shibboleth facilitates exchange of attributes in a trusted manner between Identity Providers and Service Providers
- Examples of attributes – range from totally anonymous to personal information
 - Member of University of Jonestown
 - Member of the Biology Faculty at the University of Jonestown
 - John Smith, a professor in the Biology Faculty at the Springfield campus of University of Jonestown who's eyes are blue and hair is grey

Attribute Policies

- Attribute Release Policy (ARP) governed by Identity Provider, and eventually by users themselves
 - May vary per target Service Provider
- Attribute Acceptance Policy (AAP) set by Service Provider
 - Defines which credentials the SP needs to provide access to the Service

Strong Privacy Protection

- Service-provider and user-level Attribute Release Policies
- Non-personally identifying attributes may be sufficient to grant access to services
- “Targeted ID” mechanism
 - Provides a unique, persistent identifier which is specific to an individual user accessing a specific SP from a specific IdP
 - Allows personalization while preventing aggregation of usage information across different SPs.