Project Shibboleth: Implementing Federated Identity Management

Keith Hazelton
University of Wisconsin-Madison
Internet2 MACE member

With thanks to Michael Gettes of Duke University (gettes@duke.edu)

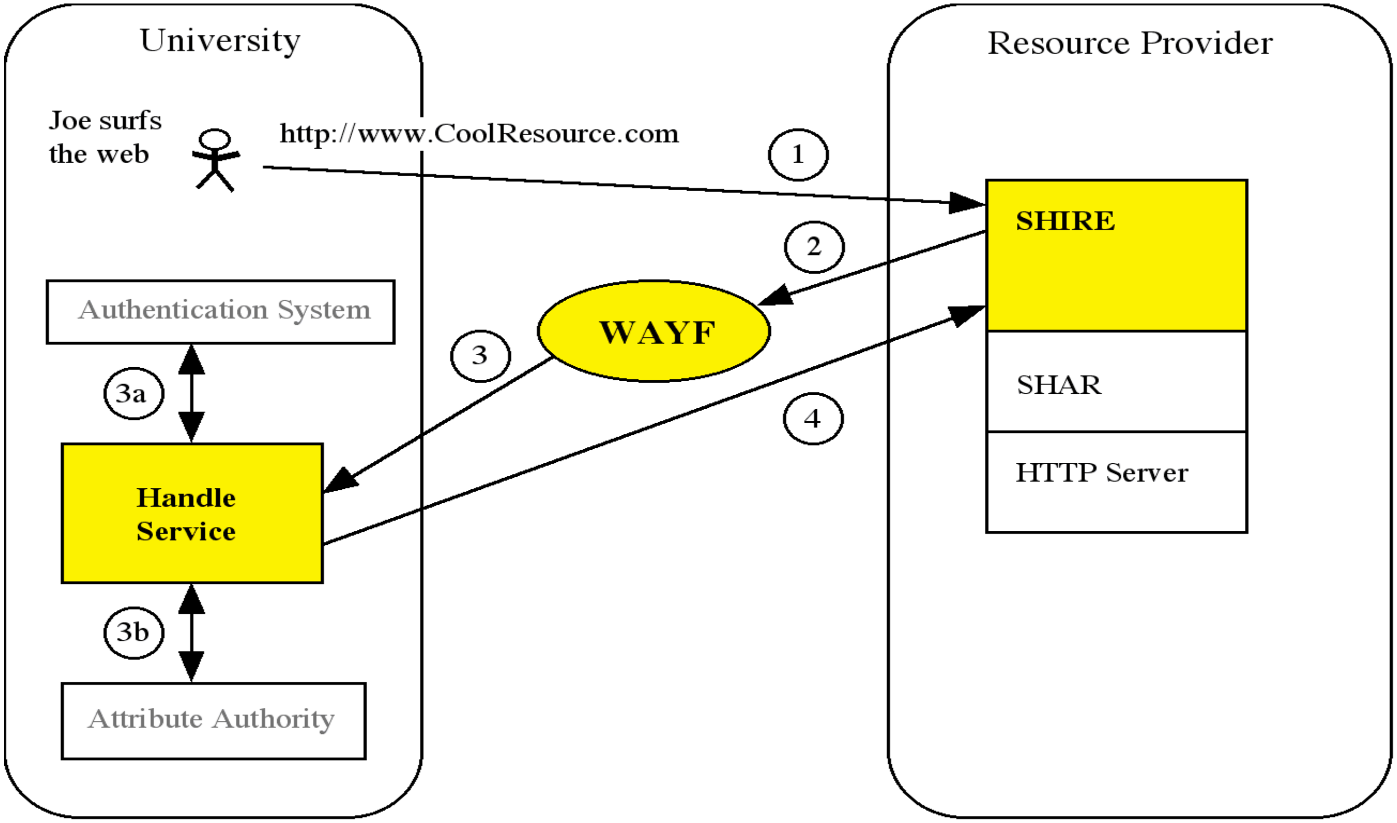
Shibboleth

- *A word which was made the criterion by which to distinguish the Ephraimites from the Gileadites. The Ephraimites, not being able to pronounce sh, called the word sibboleth. See --Judges xii.*
- *Hence, the criterion, test, or watchword of a party; a party cry or pet phrase.*

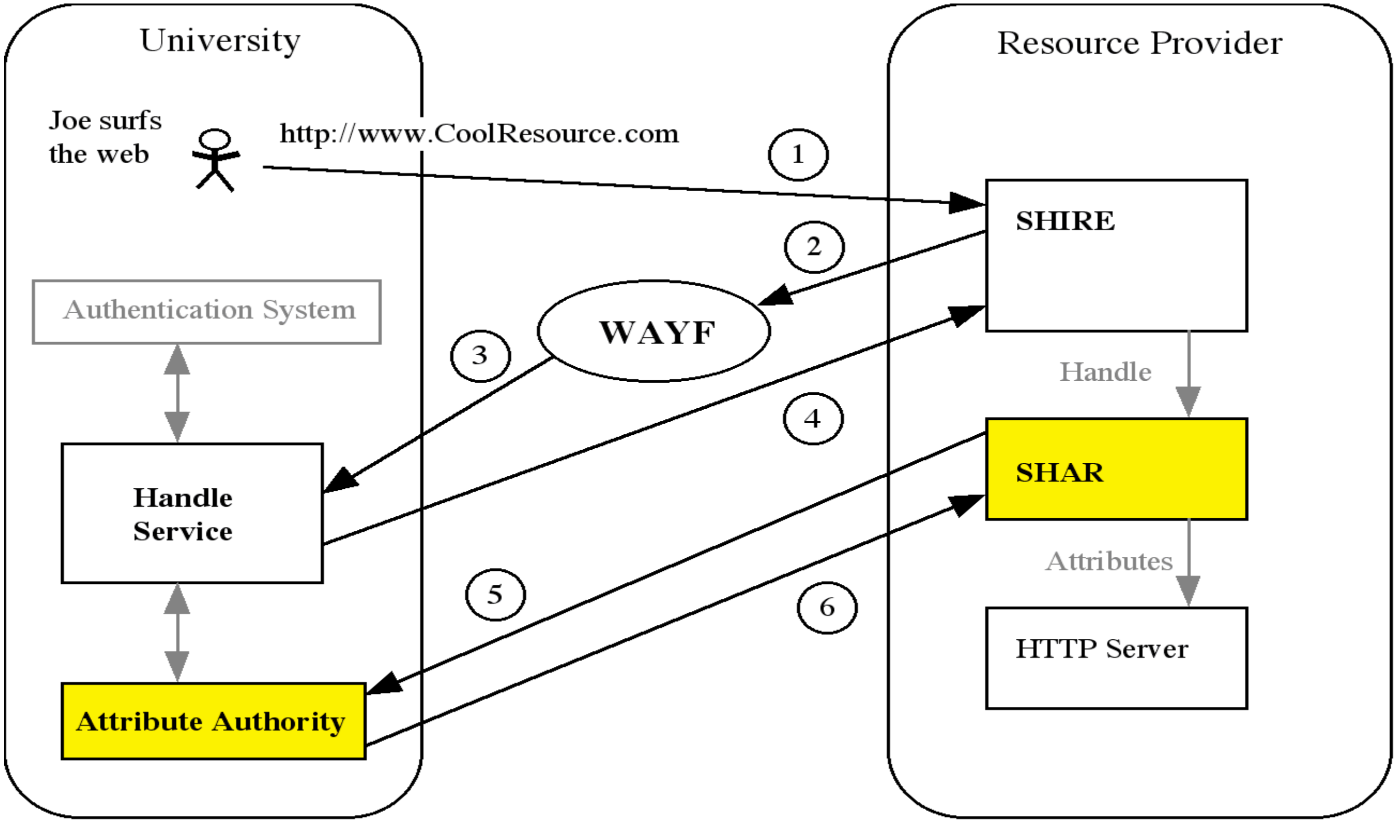
  - *Webster's Revised Unabridged Dictionary (1913):*

- http://shibboleth.internet2.edu

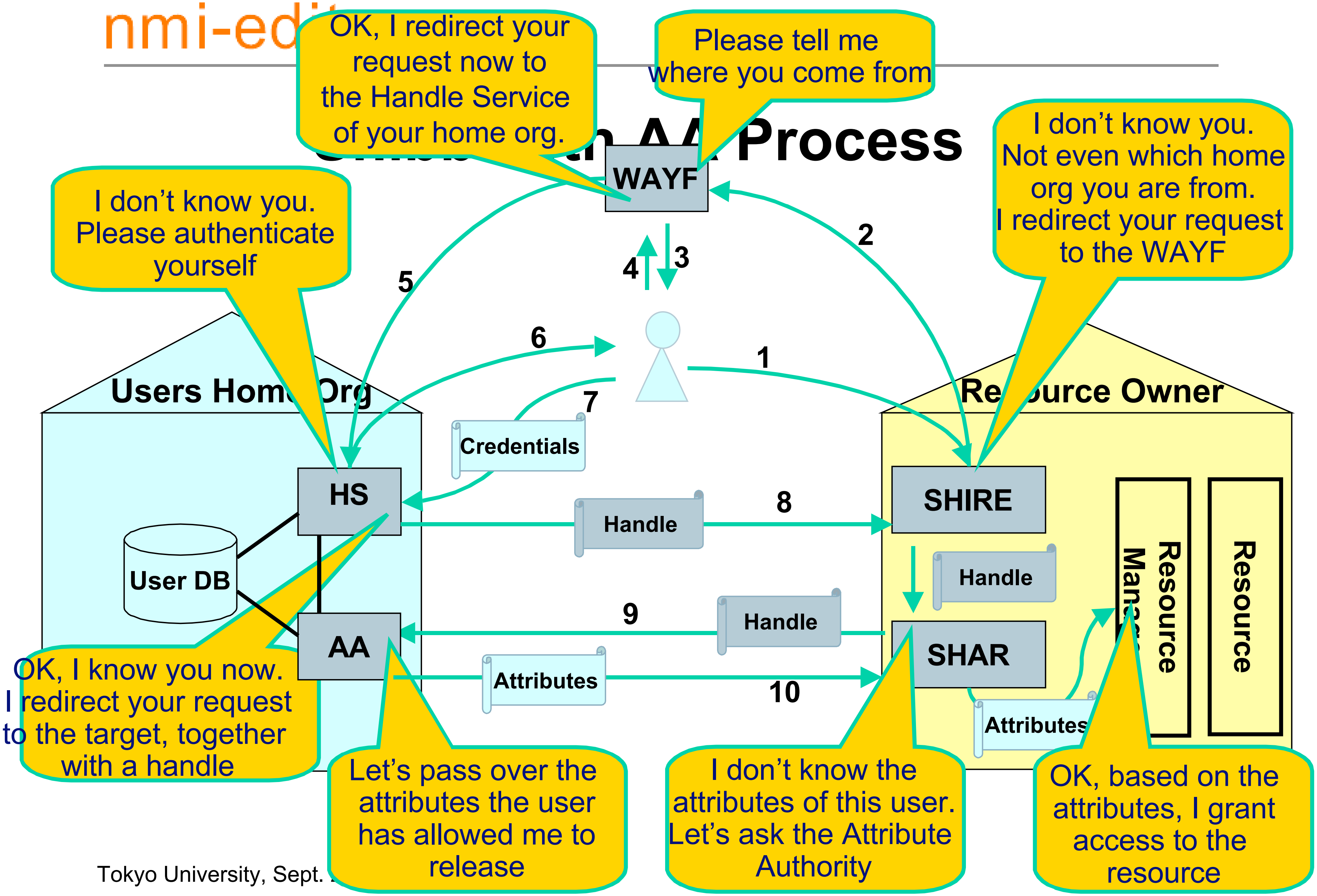
Establishing a User Context



Getting Attributes and Determining Access



h AA Process



Please tell me where you come from

OK, I redirect your request now to the Handle Service of your home org.

I don't know you. Not even which home org you are from. I redirect your request to the WAYF

I don't know you. Please authenticate yourself

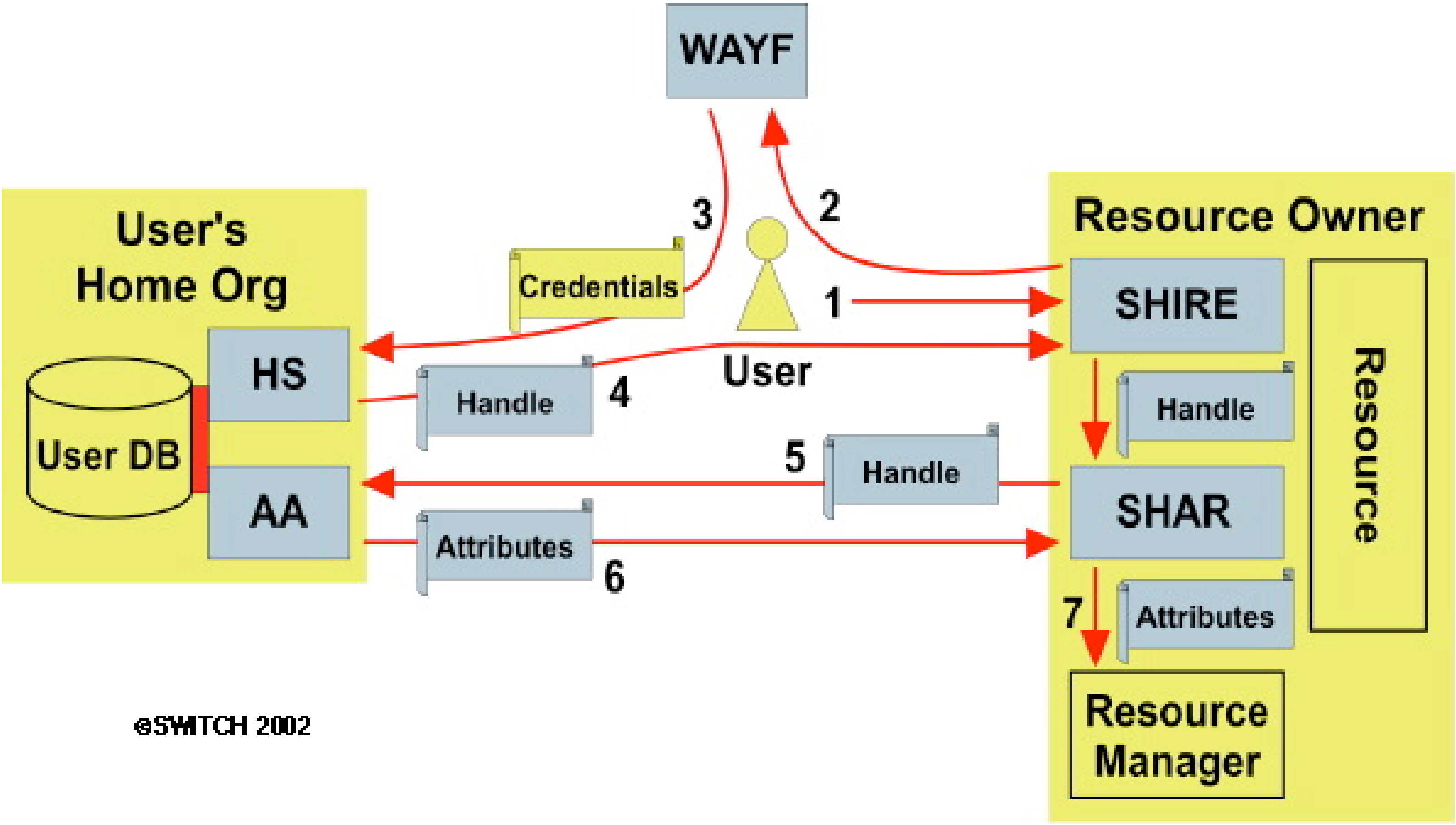
OK, I know you now. I redirect your request to the target, together with a handle

Let's pass over the attributes the user has allowed me to release

I don't know the attributes of this user. Let's ask the Attribute Authority

OK, based on the attributes, I grant access to the resource

Shibboleth Architecture



©SWITCH 2002

Milestones

- Project formation - Feb 2000 Stone Soup
- Process - began late summer 2000 with bi-weekly calls to develop scenario, requirements and architecture.
- Linkages to SAML established Dec 2000
- Architecture and protocol completion - Aug 2001
- Design - Oct 2001
- Alpha-1 release – April 24, 2002
- OpenSAML release – July 15, 2002
- v0.7 Shibboleth released Nov 25, 2002
- v1.0 July 2003
- v1.1 August 2003

Course Management (e-Learning) Early Adopters

- WebCT
- Webassign
- Blackboard (Demonstrated April, 2003)
- OKI

The Library Pilots

- Explore and evaluate the utility of the Shibboleth model using attributes to control access to licensed resources
- Identify problems and issues with this approach
  - How well do existing licenses map to attributes?
  - Library “walk-in” customers
- Identify and address Shib deployment issues for campuses AND for vendors
- Explore new possibilities, including role-based access controls
- Completed in August, 2003. Virtually all participants moving on to deploy production systems

Campus Participants

- Carnegie Mellon
- Columbia
- Dartmouth
- Georgetown
- London School of Economics
- New York Unv.
- Ohio State

- Others coming on

Penn State

U. Colorado

U. Michigan

U. Washington

U. Wisconsin - Madison

UCOP (U. California System)

U.Texas Health Science Center
at Houston

Vendor Participants

- EBSCO
- ~ Elsevier
- OCLC
- Sfx (Ex libris)
- JSTOR
- McGraw Hill eBooks
- Innovative (III)

- Consortial efforts: WRLC, Athens, …

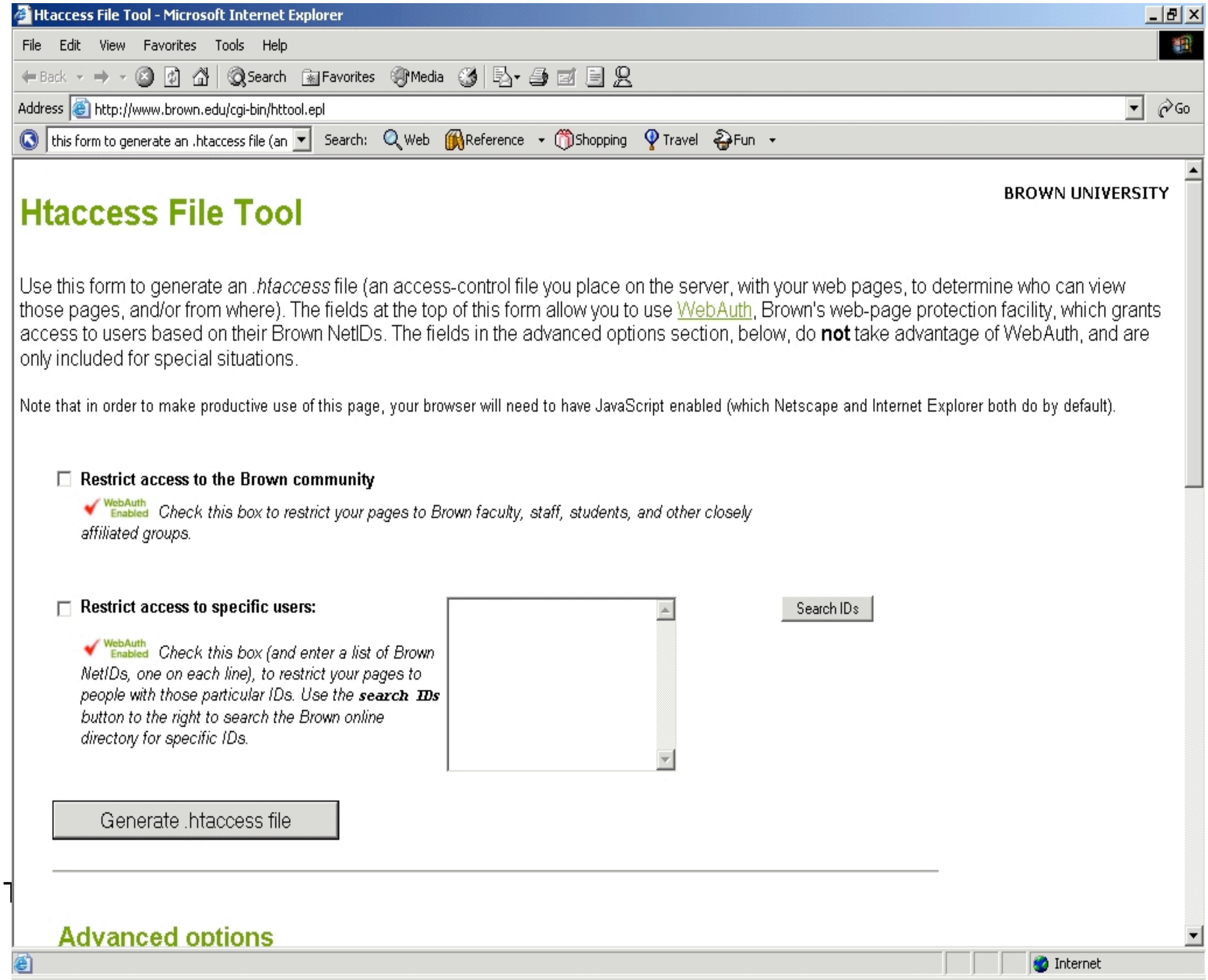
Shibboleth Deployment Issues

- Access Issues
  - Kiosks and walk-ins
  - logins for on-campus use
- Licensing issues
  - reconciling license structures with directory structures
  - system and consortial issues
  - mitigating disintermediation
- Functional issues
  - handling Shibbed and non-Shibbed resources
  - roll-out strategies
  - entitlements vs attributes
  - what attributes to pass
  - how to structure the attribute name space

Next steps

- Convergence with other efforts (PAPI, Permis, A-Select, etc)
- Shibboleth used as a WebISO solution, the N-Tier problem
- What is a Federation? How do we define it?
- Sub-Fed, Fed Clusters, Super Federations
- Shibboleth the architecture vs Shibboleth the web service
- Shibboleth the technology vs InCommon the trust model
- Federated Digital Rights Management
- Federated P2P
- Privacy Management Systems – see http://www.ischool.washington.edu/shibbui/index.html
- Personal Information Managers – see http://www.brown.edu/cgi-bin/httool.epl

Personal Resource Manager


Htaccess File Tool - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.brown.edu/cgi-bin/httool.epl
Go
this form to generate an .htaccess file (an
Search: Web Reference Shopping Travel Fun
BROWN UNIVERSITY
Internet

Htaccess File Tool

Use this form to generate an *.htaccess* file (an access-control file you place on the server, with your web pages, to determine who can view those pages, and/or from where). The fields at the top of this form allow you to use WebAuth, Brown's web-page protection facility, which grants access to users based on their Brown NetIDs. The fields in the advanced options section, below, do **not** take advantage of WebAuth, and are only included for special situations.

Note that in order to make productive use of this page, your browser will need to have JavaScript enabled (which Netscape and Internet Explorer both do by default).

□ **Restrict access to the Brown community**

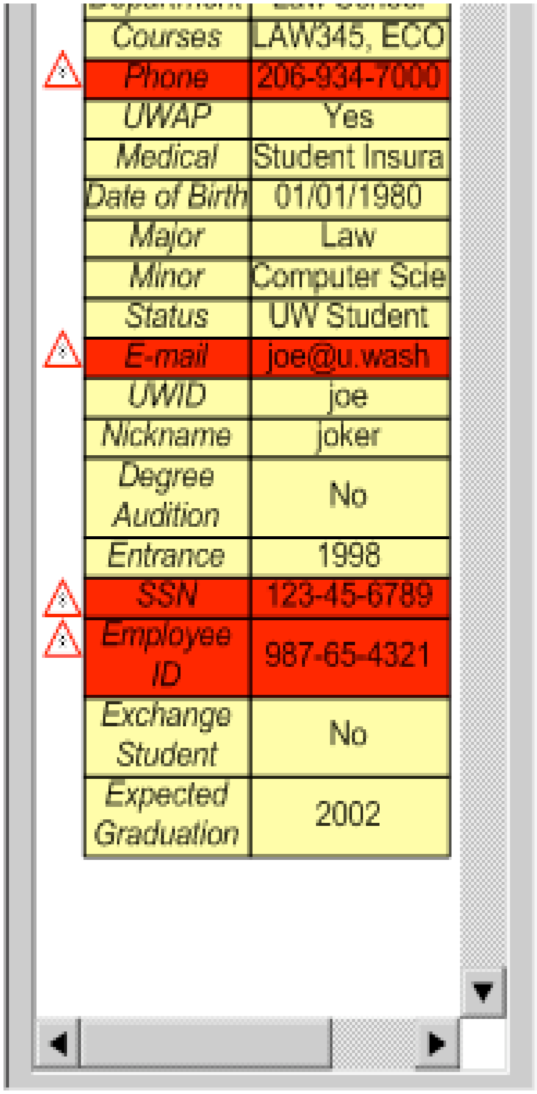
✓ WebAuth Enabled *Check this box to restrict your pages to Brown faculty, staff, students, and other closely affiliated groups.*

□ **Restrict access to specific users:**

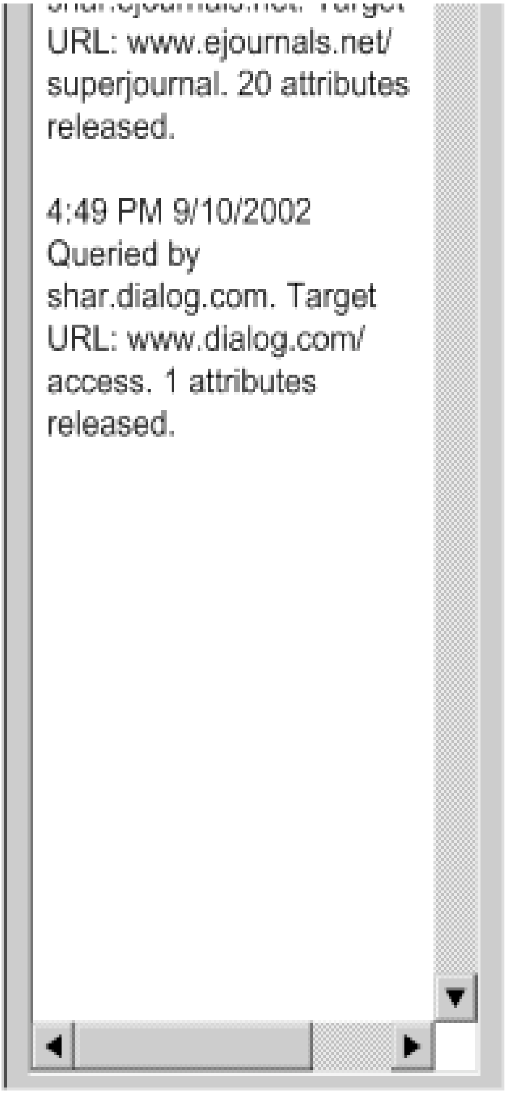
✓ WebAuth Enabled *Check this box (and enter a list of Brown NetIDs, one on each line), to restrict your pages to people with those particular IDs. Use the* ***search IDs*** *button to the right to search the Brown online directory for specific IDs.*

Advanced options

Privacy Management Systems



	Courses	LAW345, ECO
⚠	Phone	206-934-7000
	UWAP	Yes
	Medical	Student Insura
	Date of Birth	01/01/1980
	Major	Law
	Minor	Computer Scie
	Status	UW Student
⚠	E-mail	joe@u.wash
	UWID	joe
	Nickname	joker
	Degree Audition	No
	Entrance	1998
⚠	SSN	123-45-6789
⚠	Employee ID	987-65-4321
	Exchange Student	No
	Expected Graduation	2002



URL: www.ejournals.net/
superjournal. 20 attributes
released.

4:49 PM 9/10/2002
Queried by
shar.dialog.com. Target
URL: www.dialog.com/
access. 1 attributes
released.

Swiss Education and Research Network Shibboleth Demo

- http://www.switch.ch/aai/demo/
- http://bbcommerce.blackboard.com/webapps/portal/frameset.jsp

Lionshare: Academic P2P and Shibboleth

- http://p2p.libraries.psu.edu/

Shibboleth Documentation

- http://shibboleth.internet2.edu/#Documentation

Shib source cvs (web interface)

- http://marsalis.internet2.edu/cgi-bin/viewcvs.cgi/#dirlist