Project Shibboleth
Update, Demonstration and Discussion

Michael Gettes (gettes@Duke.EDU)

May 20, 2003

TERENA Conference, Zagreb, Croatia

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):

Stage 1 - Addressing Three Scenario's

Member of campus community accessing licensed resource

- Anonymity required

Member of a course accessing remotely controlled resource

- Anonymity required

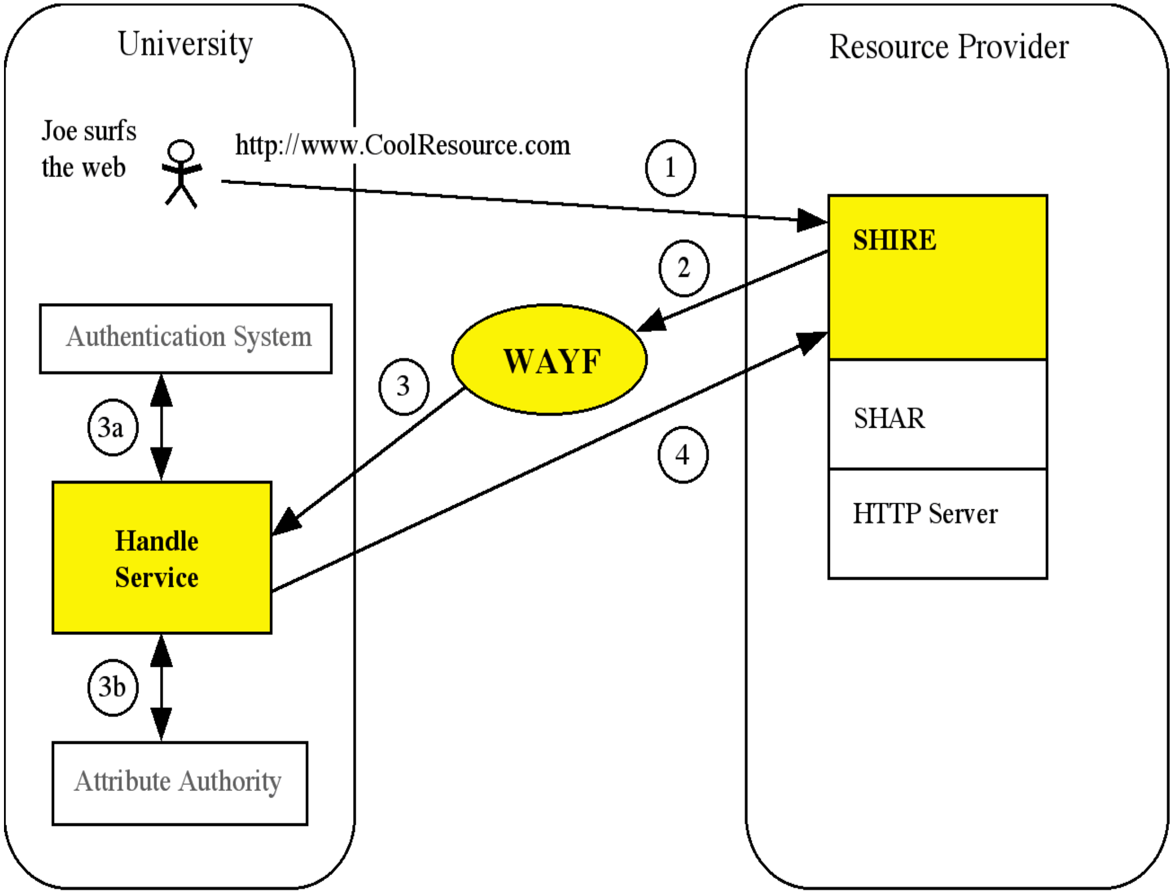
Member of a workgroup accessing controlled resources

- Controlled by unique identifiers (e.g. name)

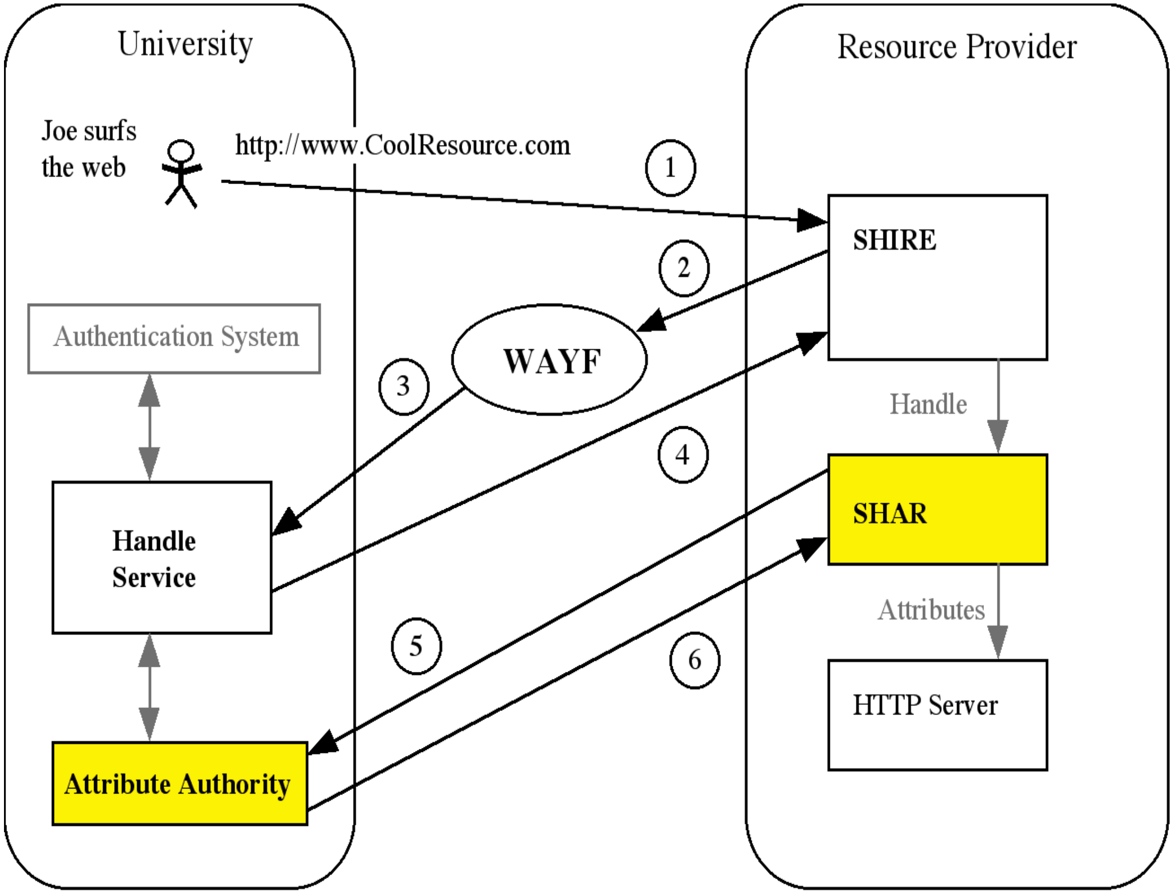
Taken individually, each of these situations can be solved in a variety of straightforward ways.

Taken together, they present the challenge of meeting the user's reasonable expectations for protection of their personal privacy.

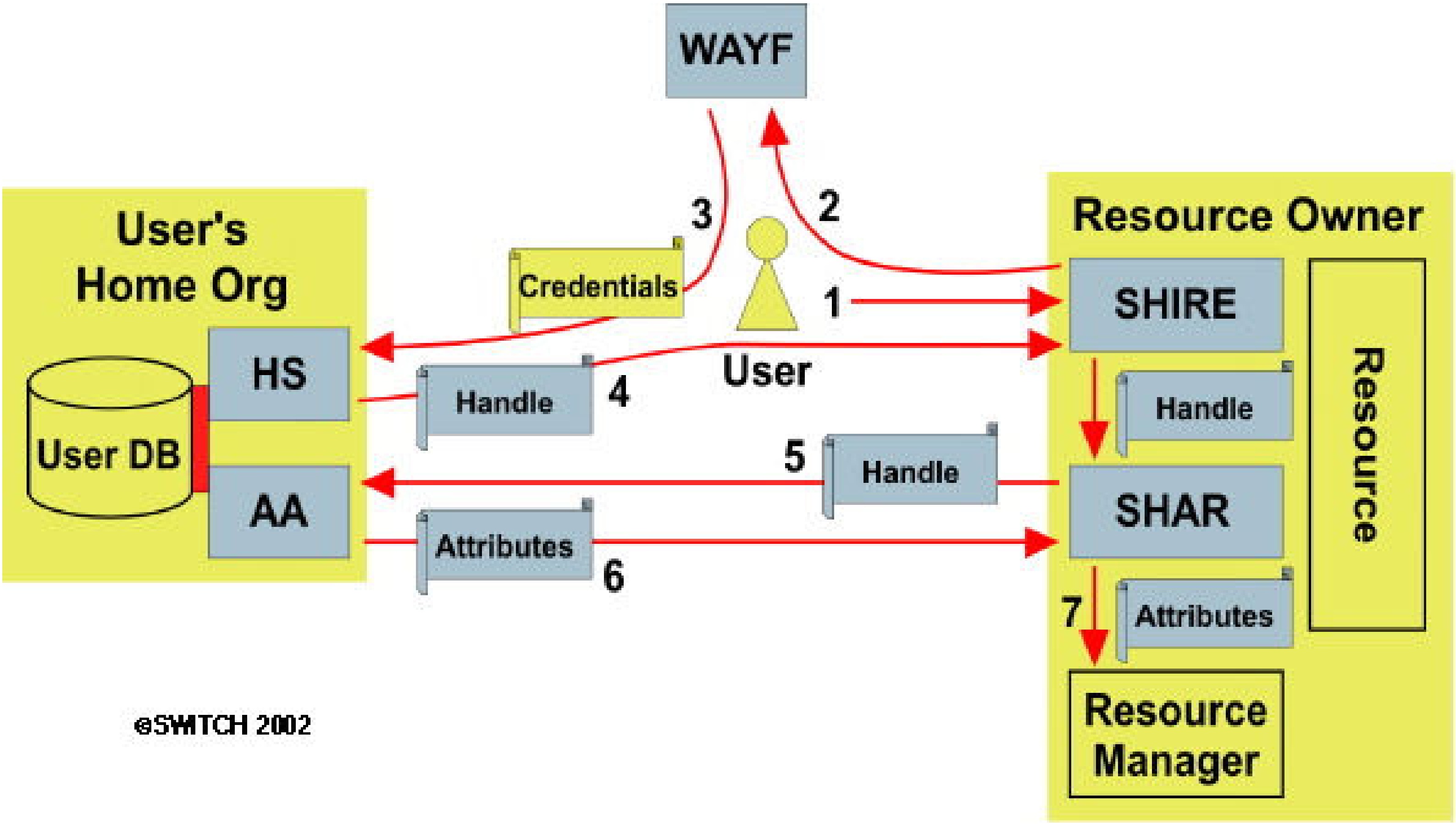
Establishing a User Context



Getting Attributes and Determining Access

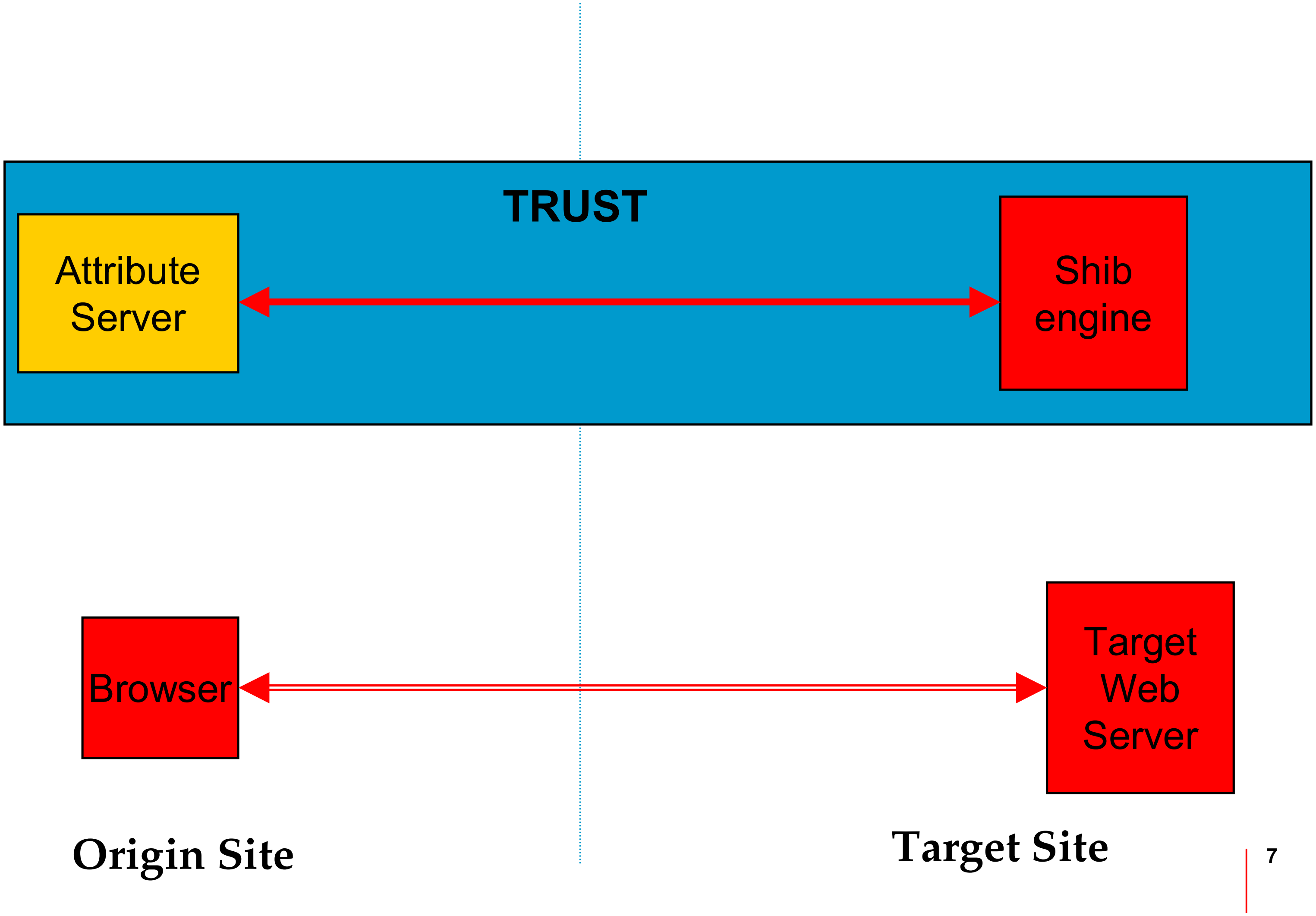


Shibboleth Architecture



©SWITCH 2002

Shibboleth Architecture -- Managing Trust



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

Coding began - Nov 2001

Alpha-1 release – April 24, 2002

OpenSAML release – July 15, 2002

v0.7 Shibboleth released Nov 25, 2002

v0.8 March 1, 2003

v1.0 May 2003 (end of month)

v1.1 conversations ruminating; v1.2 may be the plateau

Code status

v0.8 released March 2003 (coding teams – MIT, Columbia, Ohio State, CMU); v1.0 due out April 10

v0.7 much easier to install than alpha's. C/C++ only on origin. Java still on target. Relatively safe to deploy and experiment

Release issues – platform dependencies, fragile Apache components, binaries vs source, etc…

v0.7 to v0.8

- *new features – ARP's redone, added robustness*
- *timeframes – march 1, 2003 general release*

V0.8 to 1.0 – SAML 1.1 support, bug fixes and re-packaging

Course Management Early Adopters

WebCT

Webassign

Blackboard (Demonstrated April, 2003)

OKI

The Library Pilots

- *Explore and Evaluate the utility of the Shibboleth model (attributes) for controlling 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 deploy issues for campuses AND for vendors*
- *Explore new possibilities, including role-based access controls*

Campus Participants

Carnegie Mellon

Columbia

Dartmouth

Georgetown

London School of Economics

New York Unv.

Ohio State

Penn State

U. Colorado

U. Michigan

U. Washington

U. Wisconsin - Madison

UCOP (U. California System)

U.Texas Health Science Center
at Houston

Others coming on

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*

A Quick Demonstration

[Shib Demo Site]

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 Club Shib the trust model

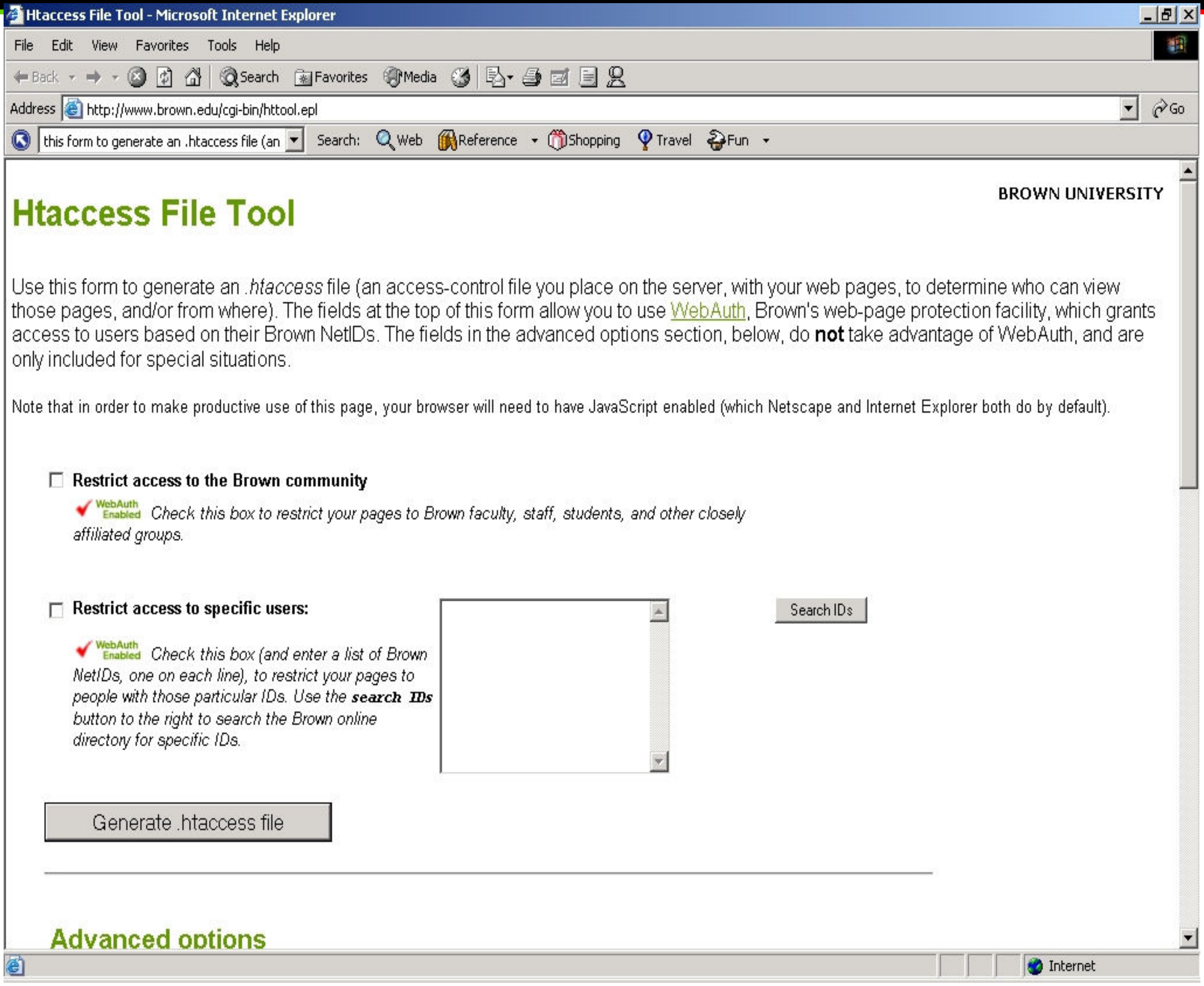
Federated Digital Rights Management

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
Internet

Htaccess File Tool

BROWN UNIVERSITY

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**

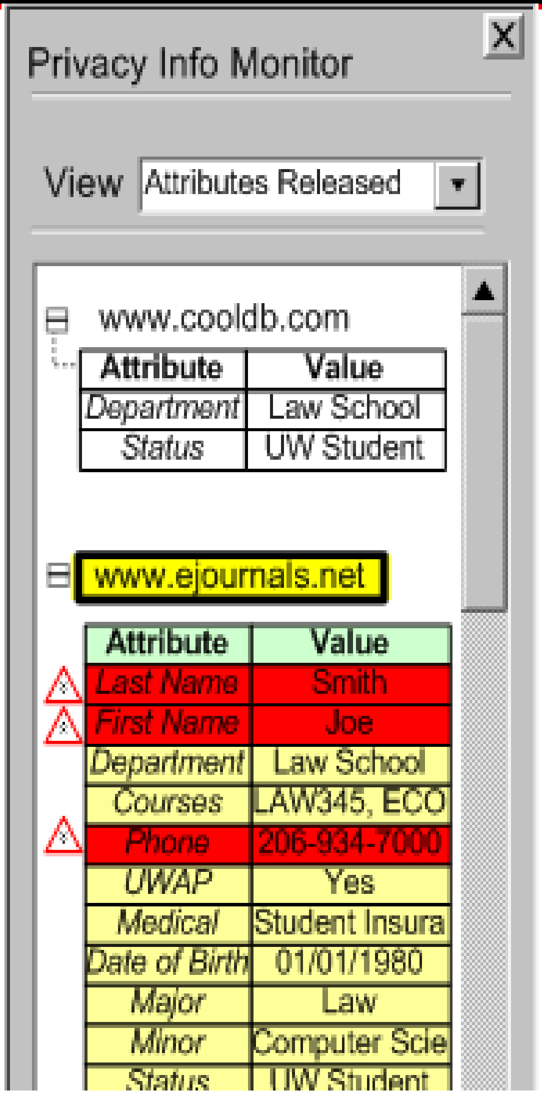
✓ WebAuth Enabled *Check this box to restrict your pages to Brown faculty, staff, students, and other closely affiliated groups.*

☐ **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



Privacy Info Monitor

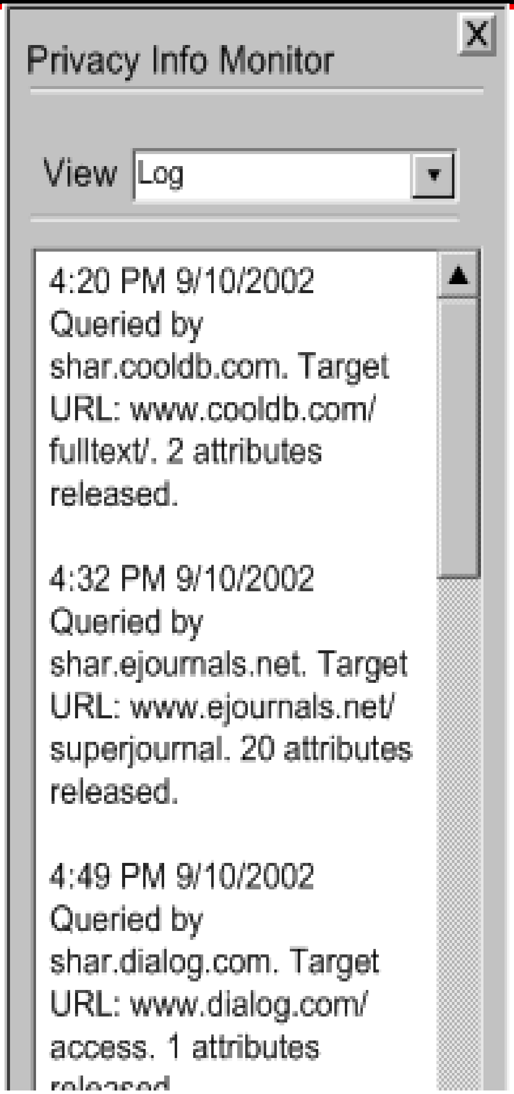
View: Attributes Released

www.cooldb.com

Attribute	Value
Department	Law School
Status	UW Student

www.ejournals.net

Attribute	Value
⚠ *Last Name*	Smith
⚠ *First Name*	Joe
Department	Law School
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



Privacy Info Monitor

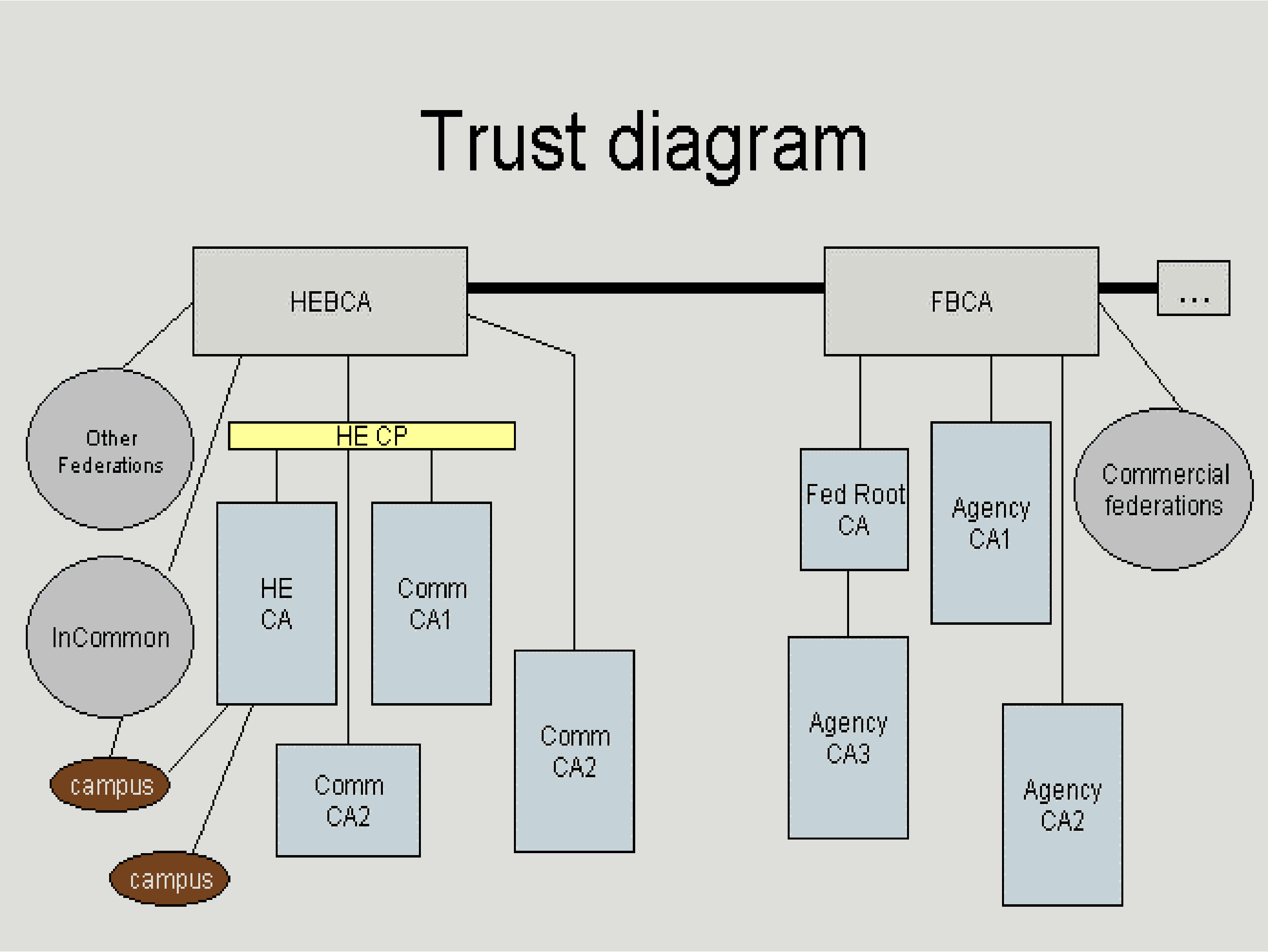
View: Log

4:20 PM 9/10/2002 Queried by shar.cooldb.com. Target URL: www.cooldb.com/fulltext/. 2 attributes released.

4:32 PM 9/10/2002 Queried by shar.ejournals.net. Target 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

Overall Trust Fabric


Trust diagram
HEBCA
FBCA
...
Other Federations
HE CP
InCommon
HE CA
Comm CA1
campus
campus
Comm CA2
Comm CA2
Fed Root CA
Agency CA1
Commercial federations
Agency CA3
Agency CA2