Identity and Access Management for Federated Resource Sharing: Shibboleth Stories

http://arch.doit.wisc.edu/keith/apan/apanShib-060122-01.ppt

Keith Hazelton (hazelton@doit.wisc.edu)
Sr. IT Architect, University of Wisconsin-Madison
Internet2 Middleware Architecture Committee for Education (MACE)

APAN, Tokyo, 22-Jan-06

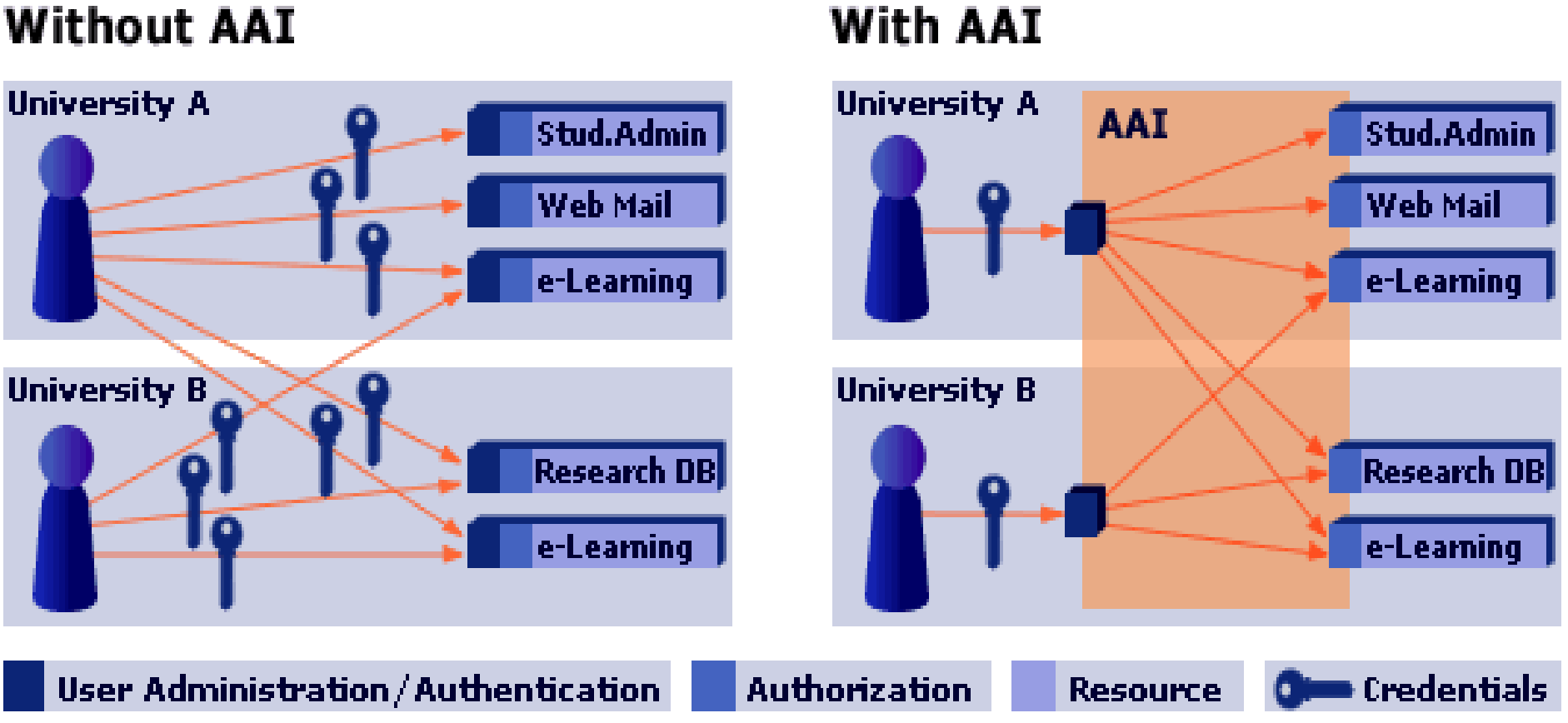
Topics

- http://arch.doit.wisc.edu/keith/apan/apanShib-060122-01.ppt
- Thesis: Growing adoption of SAML for AuthNZ between parties in Education & Research
- SAML & Shibboleth
- Evidence for thesis
  - NRENs and licensed resource providers
  - Beijing University / Harvard / U Wisconsin: Collaborative Development of the China History Biographical Database
- Shibboleth, SAML, WS-*, Grids: Coming developments

Security Assertion Markup Language

- SAML (OASIS Security Services TC)
  - 1.1 and 2.0 ratified
- Support for end-to-end, application-level security
  - Complements transport- and message-level security
  - XML schema around authentication and authorization
- Addresses a key requirement in federated environments
  - One (or more) Identity Provider (IdP) parties asserting Authentication/Attribute/Authorization information
  - Different party, a service provider (SP), relying on this information to provide a service or access to a resource

The federated access scenario
SWITCH AuthN/AuthZ Infrastructure (AAI) Site



Shibboleth: A SAML Implementation for Research & Education

- Developed by Internet2 with assistance from NSF
- Current version: Shibboleth 1.3, supports SAML 1.1
- Shibboleth is a software suite implementing SAML
- It is *also* a profile of SAML (profiles support interop.)
- It is *also* an active global community engaged in open source development and support
- http://shibboleth.internet2.edu

Evidence for the thesis: SHIB / Athens

- Athens: UK-wide service
  - Managing higher ed <=> vendor licenses for access to digital resources
  - Providing a shared authentication service for all UK higher ed users;
- Joint Information Services Committee (JISC) decision to shift from proprietary AuthN to Shib

Evidence for the Thesis: SHIB / Athens

- EduServ service provider currently offers an Athens-Shib gateway (bi-directional)
- JISC rewriting contracts: Vendors must be shib service providers at contract renewal.
- Transition to be complete by 1/1/2007

Evidence for the Thesis: BECTA

- Supports IT needs of K-12 in UK
- 3,000,000 users
- Now recommending adoption of Shibboleth for Federated Identity and Access Management
- http://www.becta.org.uk/corporate/display.cfm?section=22&id=4665

More evidence: Europe/Australia/US NREN consortium: Vendor resources as Shibboleth SPs

- Finland, Denmark, Germany Switzerland Netherlands, Belgium France Spain UK, Australia, US; Discussions w. Greece, Hungary,
- NREN-scale Shib feds in test or production
- Coordinating approaches to vendors on “Shibbing” their resources

Beijing University / Harvard / U Wisconsin: China History Biographical Database

- Well-established international collaborative to maintain and expand a database of tens of thousands of historical figures from China's imperial past.
- Currently exploring possible shift from file exchange model to federated application model
- Exploratory Shibboleth pilot project underway

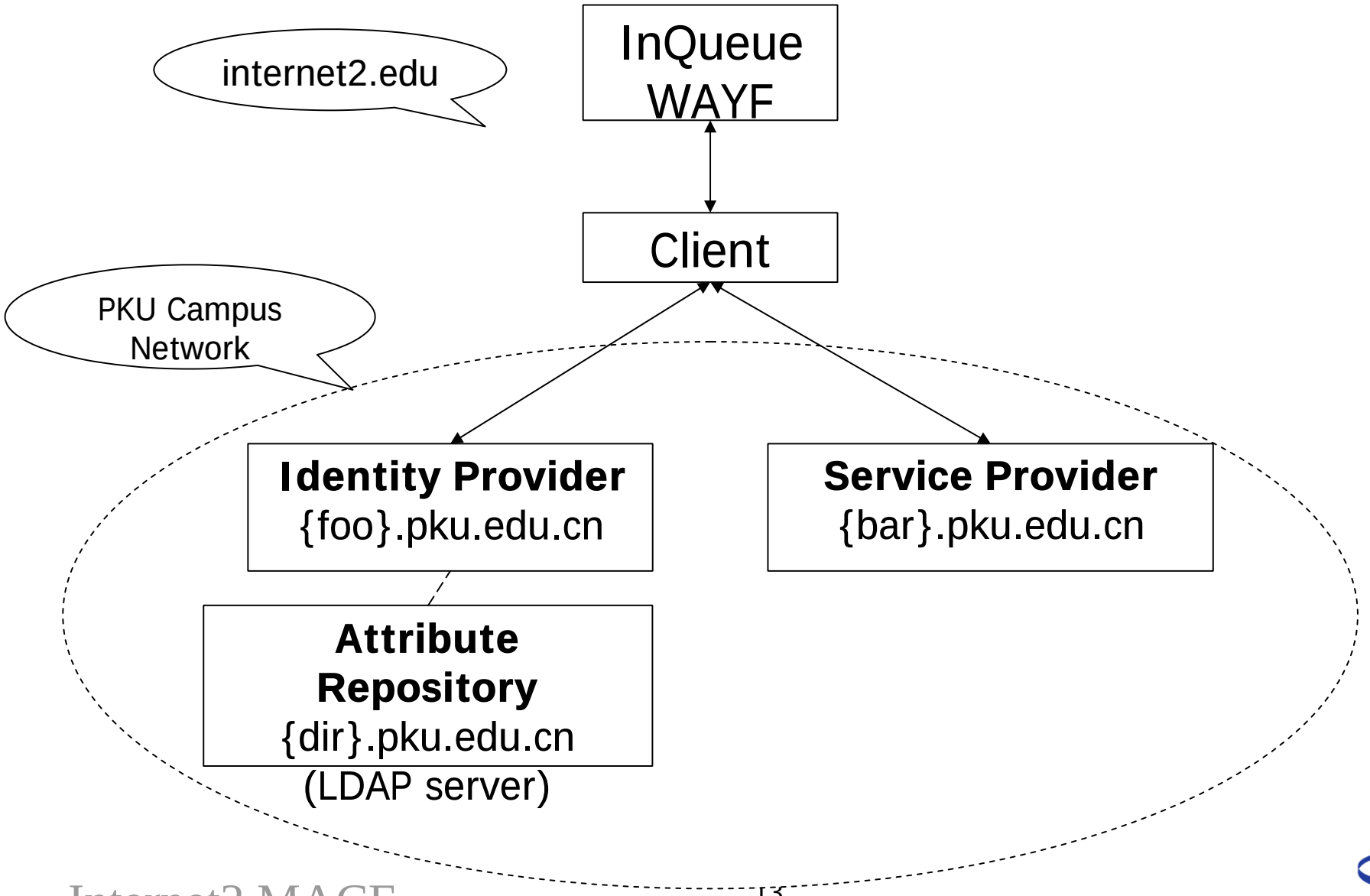
Beijing University / Harvard / U Wisconsin: China History Biographical Database

- In pilot, content experts at Beijing University (北大, PKU) would access:
- Shib-protected Web applications at Harvard that query/update the database
- PKU would be the Identity Provider
- Service Provider would be Harvard
  - PHP/MySQL app running under Apache/Tomcat

Shibboleth at Beijing University (PKU)

- Slides courtesy of PKU sponsor, Prof. ZHANG Bei (张蓓)
- Initial contacts at APAN in Taipei in August
- Work began in earnest after CANS meeting in December in Shenzhen

A glance at PKU Shibboleth



PKU in InQueue

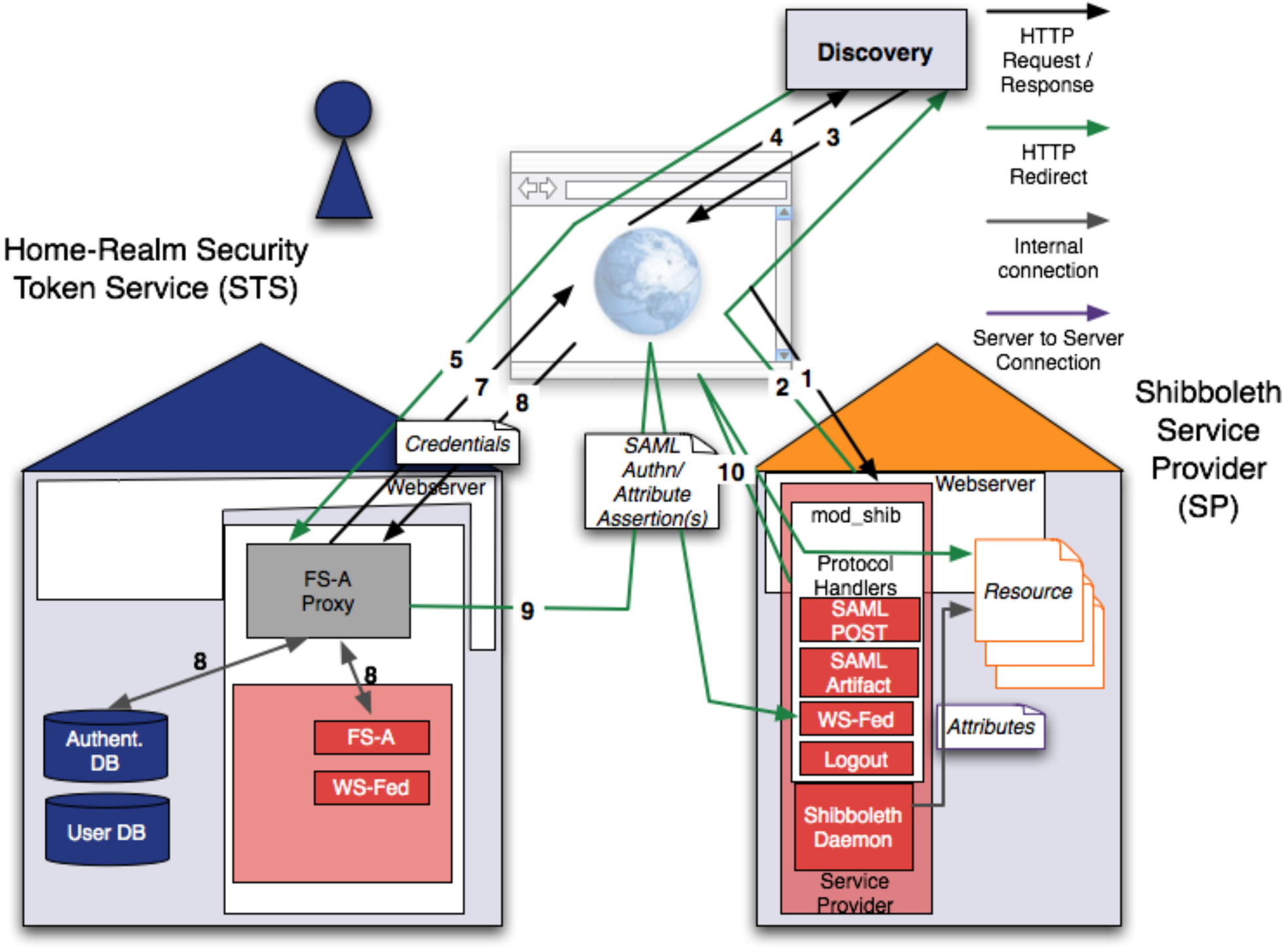
- Both our IdP and SP have joined InQueue of Internet2
- Our IdP has been successfully tested with https://wayf.internet2.edu/InQueue/sample.jsp
- To authenticate with our IdP, choose “Peking University Test Install” on the InQueue WAYF service page
- The redirection of client from SP to IdP can go with/without WAYF
- Currently working on fully utilizing the attribute exchange mechanisms provided by Shibboleth

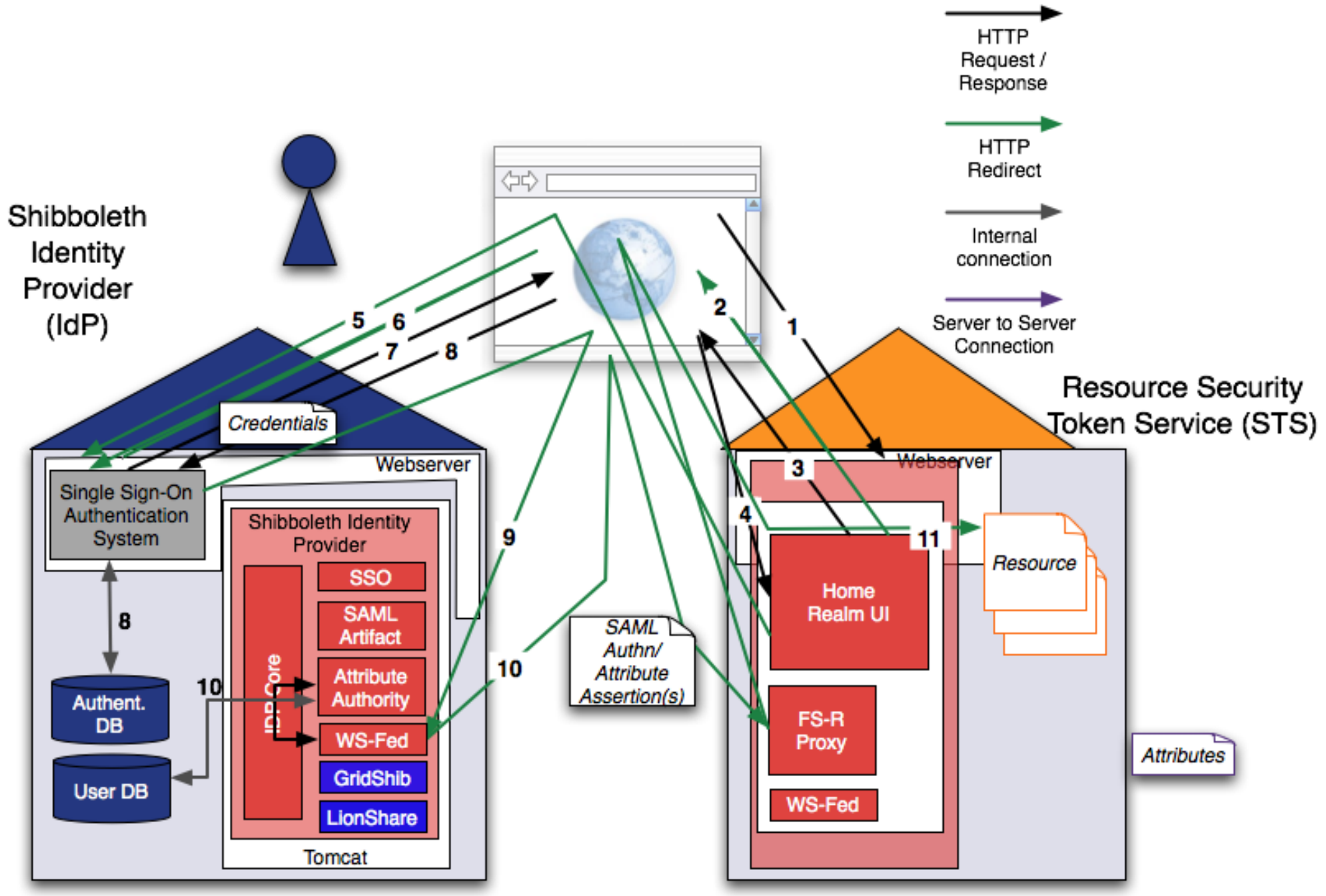
Future steps at PKU

- Configure IdP to authenticate end-users with our Web SSO solution
- Deploy Shibboleth within PKU
- Co-operate with other educational institutions
- Establish a federation within CERNET
  - Provide membership management
  - Set up our own WAYF service

Shibboleth, SAML, WS-*, Grids: Coming attractions

- Initial MS federation support available in Active Directory Federation Services (ADFS)
- Essentially a WS-Sec, WS-Fed profile, but not published
- A Shib-ADFS gateway is in Beta
  - Shib adds an end-point in IdP that can interoperate with a MS ADFS system
  - Communicates via WS-Security
  - ADFS components comparable to Shib IdP & SP
  - Use Shib IdP in conjunction with ADFS SP & vice-versa


Discovery
HTTP Request / Response
HTTP Redirect
Internal connection
Server to Server Connection
Home-Realm Security Token Service (STS)
Shibboleth Service Provider (SP)
1
2
3
4
5
7
8
8
8
9
10
Credentials
SAML Authn/ Attribute Assertion(s)
Webserver
FS-A Proxy
Authent. DB
User DB
FS-A
WS-Fed
Webserver
mod_shib
Protocol Handlers
SAML POST
SAML Artifact
WS-Fed
Logout
Shibboleth Daemon
Service Provider
Resource
Attributes


HTTP Request / Response
HTTP Redirect
Internal connection
Server to Server Connection
Shibboleth Identity Provider (IdP)
Resource Security Token Service (STS)
Credentials
Webserver
Single Sign-On Authentication System
Shibboleth Identity Provider
SSO
SAML Artifact
Attribute Authority
WS-Fed
GridShib
LionShare
IDP Core
Authent. DB
User DB
Tomcat
SAML Authn/ Attribute Assertion(s)
Webserver
Home Realm UI
FS-R Proxy
WS-Fed
Resource
Attributes
1
2
3
4
5
6
7
8
9
10
11

• Shibboleth, SAML, WS-*, Grids: Coming attractions

- Shib 2.0
  - Beta expected in May, 2006
  - Formal release by end of summer
- Will support SAML 2.0
- Will address the N-Tier problem
  - Constrained delegation model
  - Seeking to work with various standards bodies

Shibboleth, SAML, WS-*, Grids: Coming attractions

- ***OpenSAML 2.0 well underway***
- ***Shib 2.0 will have an AuthN engine because it is necessary to meet SAML 2.0 requirements***
  - ***Watch shibboleth-dev@internet2.edu mailing list for a list of features***
- ***Linking attributes from multiple identity providers***
- ***Shib 2.0 code will support Shib 1.3 endpoints***
- ***Will include a pure Java implementation***
  - ***Takes Shib beyond simple web app scenarios***

- Shibboleth, SAML, WS-*

- SAML 1.1 profile included in WS-Sec
- Interfederation gateway products available, more coming
- Demoed at Catalyst 2005
- SAML tokens included in WS-Sec payloads to carry AuthNZ information

The state of play with WS-*

- SAML in wide use in production environments
- WS-Sec is out & in use, but what of WS-*?
  - WS Trust, WS Federation in particular
  - Complexity is their hallmark

The state of play with WS-*

- WS-* Still in flux
- Open source implementations lacking
- True inter-vendor interoperability not yet within reach
  - Specifications don't provide it
  - Only profiles of specifications can
  - WS-* profiles don't yet exist

Q & A