AAI Demo Day - Shibboleth

SWITCH
The Swiss Education & Research Network

- Origin of Shib
- Status of Shib
- System architecture
- Demo
- Technologies involved
- How to implement a target site
- AAI-specific configuration
- Need to know & pitfalls
- Open issues

SWITCH aai

Origin of Shib

SWITCH
The Swiss Education & Research Network

Part of Internet2

Middleware Architecture Committee for Education (MACE)

Design goals:

- Federated administration
- Privacy
- Web-based resources

SWITCH aai

Status of Shib

SWITCH
The Swiss Education & Research Network

Latest Version: alpha 2.5

- difficult to install
- just enough functionality for a working Shib implementation

Next release: beta

- goes to first test site in the US later this week
- should be easier to install (./configure, make install)
- complete rewrite of target side, no tomcat/java anymore on target side

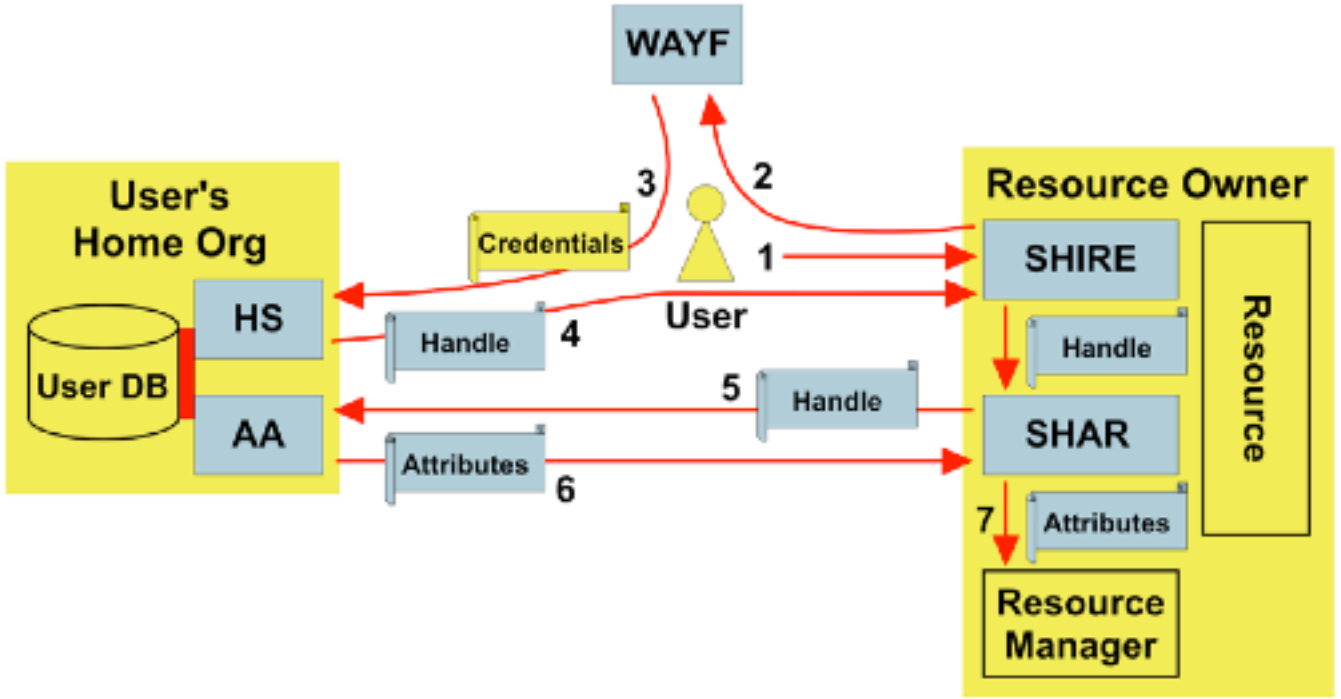
Shib v1.0: should be available on 25.10.02

SWITCH aai

System architecture

Origin site

Target site

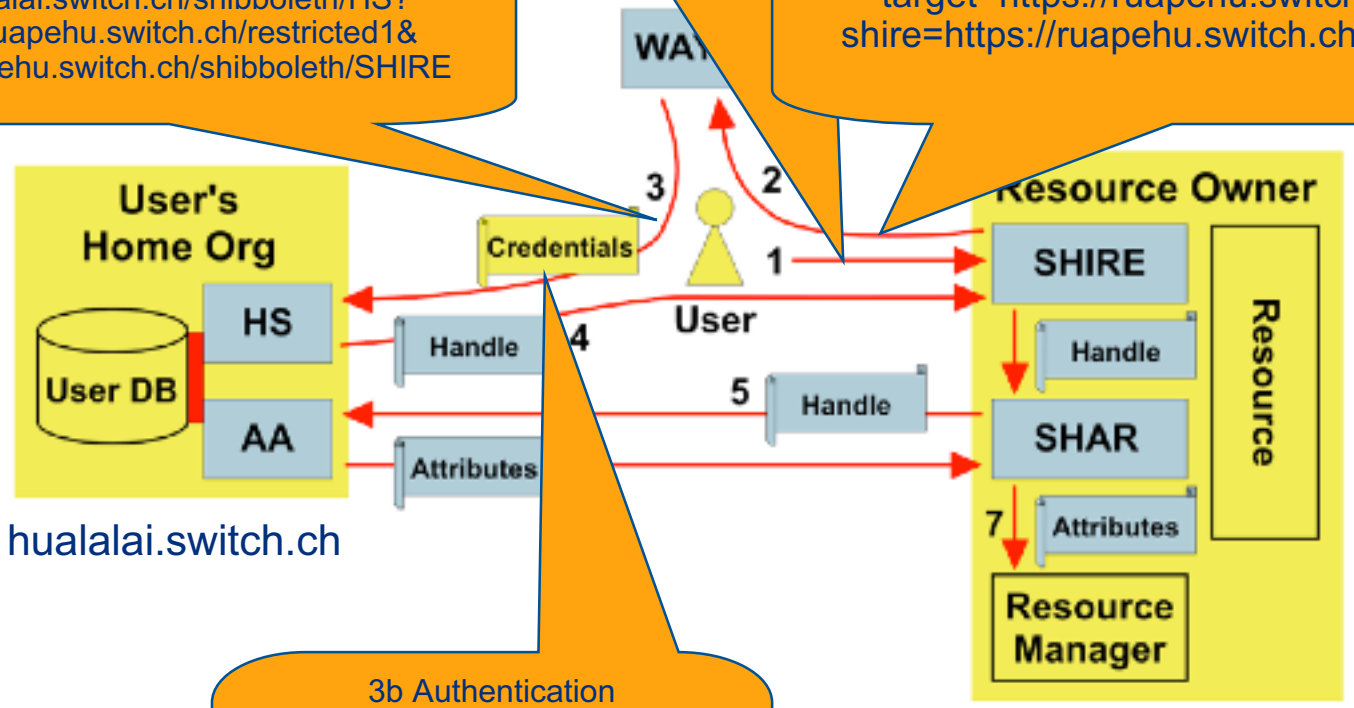


HTTP(S) calls, Part 1/2

1. https://ruapehu.switch.ch/restricted1

2. http://hualalai.switch.ch/shibboleth/WAYF?
target=https://ruapehu.switch.ch/restricted1&
shire=https://ruapehu.switch.ch/shibboleth/SHIRE

3a. http://hualalai.switch.ch/shibboleth/HS?
target=https://ruapehu.switch.ch/restricted1&
shire=https://ruapehu.switch.ch/shibboleth/SHIRE



hualalai.switch.ch

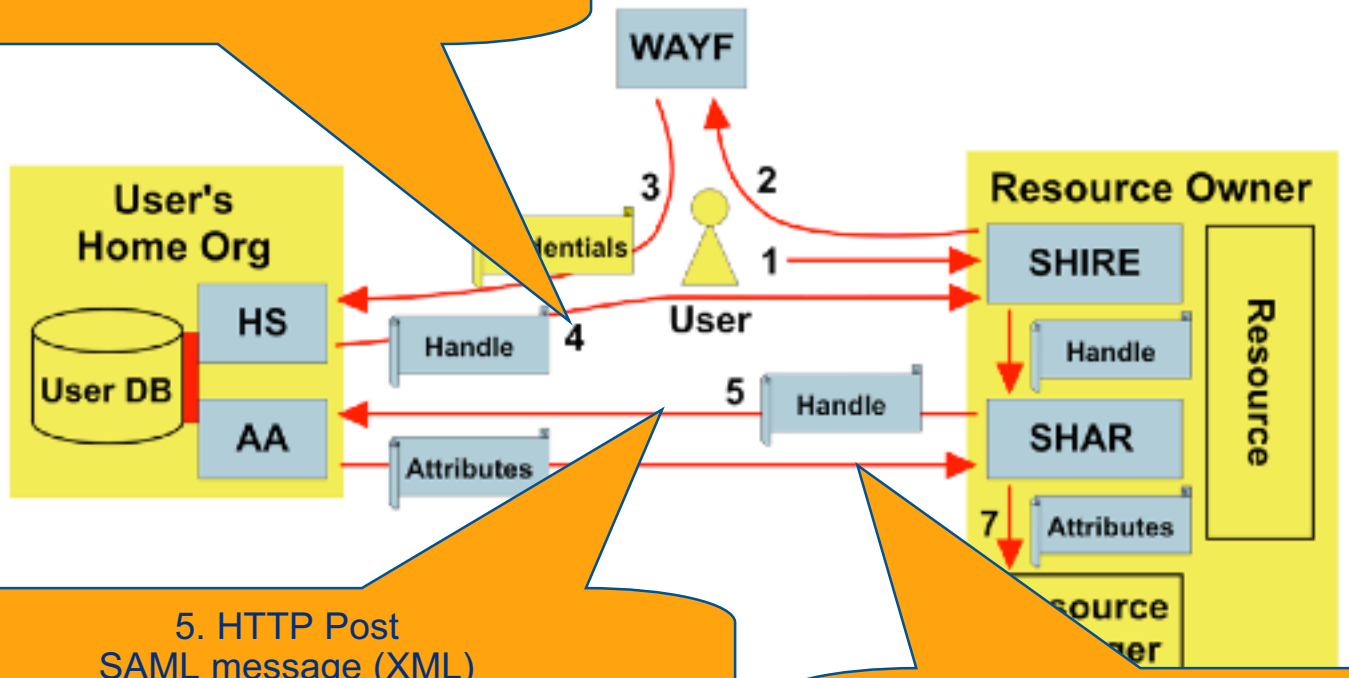
ruapehu.switch.ch

3b Authentication

HTTP(S) calls, Part 2/2

SWITCH
The Swiss Education & Research Network

4. HTTP Post
TARGET=https://ruapehu.switch.ch/restricted1
SAMLResponse=….. Handle, AA, ……

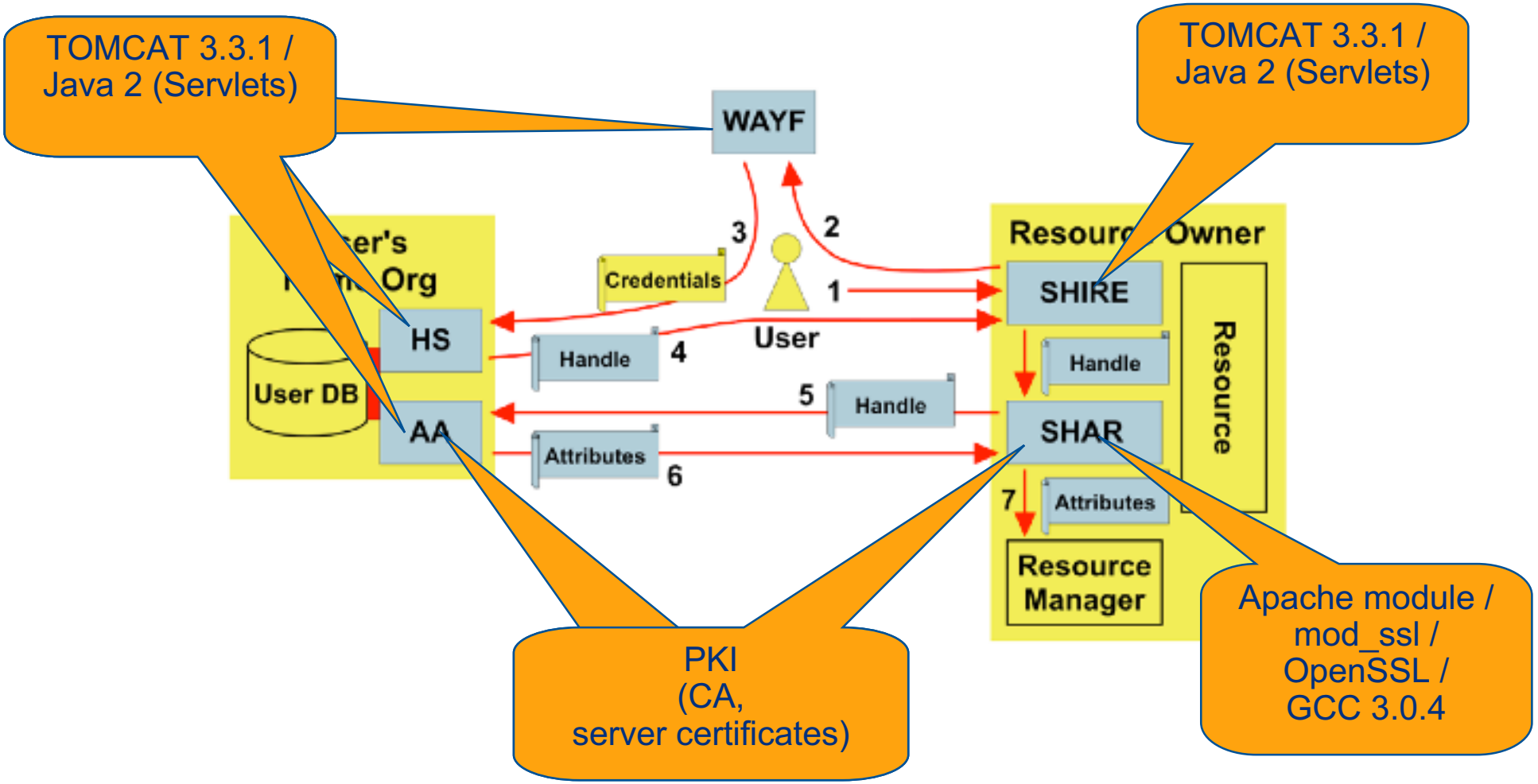


5. HTTP Post
SAML message (XML)
Attribute Query Message

6. HTTP Response
SAML message (XML)
Attribute Query Response

SWITCH aai

Technologies involved



SWITCH aai

How to implement a target site

SWITCH
The Swiss Education & Research Network

Installation

- Download Shib Distribution (http://wayf.internet2.edu/shibboleth/)
- Follow instructions in
- DEPLOY.TXT (part of shib distribution) and at
- http://hualalai.switch.ch (Installation Notes for ruapehu.switch.ch)
- For alpha 2.5 RedHat 7.2 suggested

Suggested Reading

- http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf
- http://www.internet2.edu/presentations/20020731-AdvCAMP-Cantor.ppt

SWITCH aai

AAI-specific configuration of target site 1/2

SWITCH
The Swiss Education & Research Network

SHIRE: web.xml

- registry-uri: http://hualalai.switch.ch/shibboleth/sites.xml
- ssl-only: false (optional)

SHAR: httpd.conf

- disable php4_module
- <Location /restricted1>
  AuthType shibboleth
  Require valid-user
  </Location>
- Add additional section as described in DEPLOY.TXT to httpd.conf

```
ShibCookieName shib_shib1
ShibSSLKeyFile /etc/httpd/conf/ssl.key/server.key
ShibSSLCertFile /etc/httpd/conf/ssl.crt/server.crt
ShibSSLKeyPass <whatever_password>
WAYFLocation http://hualalai.switch.ch/shibboleth/WAYF
```

SWITCH aai

AAI-specific configuration of target site 2/2

SWITCH
The Swiss Education & Research Network

PKI:

- Generate a server.key with openssl, and send CSR to aai@switch.ch
- Overwrite server.crt with the one that is signed and returned from SWITCH
- Overwrite ca_bundle.crt with the one that is downloaded or sent from SWITCH

For more details see: http://hualalai.switch.ch (Installation Notes for ruapehu.switch.ch)

SWITCH aai

Need to know & pitfalls

SWITCH
The Swiss Education & Research Network

- First call very slow (needs compilation of Java-servlets) (up to 1 min)
- Permissions of /etc/httpd/conf/ssl.* should be 755
- Remove unpatched libssl.so.0.9.6b and libcrypto.so in older Shib distributions
- Origin site and target site need to be synchronised (+/- some minutes)
- Remove php4_module from httpd.conf

SWITCH aai

Open issues

SWITCH
The Swiss Education & Research Network

- Get http://hualalai.switch.ch/shibboleth/sites.xml properly signed
- Attributes and Attribute Release Policy
- Authentication at HS/AA, e.g. with LDAP-server

SWITCH aai

Questions

SWITCH
The Swiss Education & Research Network

Q & A

SWITCH aai