Shibboleth Flows (in four slides)

User tries to contact Shib-protected app:
http://example.com/App

Three stages of the interaction:
Initiation and Discovery
AuthN Request & Response
Response Processing

Key entities are:
Service Provider (SP)
Identity Provider (IdP)
Discovery Server (DS)

By Marlena_Erdos with partial inspiration from Chris Bongaarts
Browser

User contacts app: http://example.com/App
SP catches the request: No valid session w/ browser

SP redirects to Discovery Service (DS)

(Where is this user from request)

DS asks “Where are you from?”

User selects and submits home institution

DS redirects to SP with IdP info in url

(“Here is where this user is from” response)

SP looks up endpoint info for the IdP in metadata

SP redirects to IdP; AuthN Rqst

Continued on next slide

Legend: Flows in parens () are the second half of a redirect
Shibboleth AuthN Request & Response

**Legend:** Flows in parens () are the second half of a redirect

- **IdP (Identity Provider)**
  - IdP redirects to AuthN Service
  - AuthN Service e.g. Pin2
    - Login Page
    - Login info from user
    - AuthN Service redirects to IdP w/ principal identifier
    - (Redirect with principal identifier)
  - Attribute Request
  - Attribute Response
  - IdP transforms & filters attrs
  - IdP redirects to SP: authN response w/ attrs

- **Browser**
  - AuthN Service e.g. Pin2
  - (Redirect from IdP)
  - Login Page
  - Login info from user
  - AuthN Service redirects to IdP w/ principal identifier
    - (Redirect with principal identifier)
  - Attribute Service (e.g. HU-LDAP)
    - Attribute Request
    - Attribute Response
    - IdP transforms & filters attrs
    - IdP redirects to SP: authN response w/ attrs

- **SP Module (Service Provider)**
  - SP redirects to IdP: AuthN Rqst
  - (AuthN Rqst)
  - IdP redirects to AuthN Service
  - (Redirect from IdP)
  - Login Page
  - Login info from user
  - AuthN Service redirects to IdP w/ principal identifier
  - (Redirect with principal identifier)
  - Attribute Service (e.g. HU-LDAP)
    - Attribute Request
    - Attribute Response
    - IdP transforms & filters attrs
    - IdP redirects to SP: authN response w/ attrs
  - (AuthN response w/ attrs)

- **Web Server**
  - Continued on next slide
Shibboleth Response Processing

Browser

Request to http://example.com/app flows to app w/ attrs in environment variables

App makes authZ decision; Does other processing;

App returns response page to user

Web Server

SP Module

Service Provider

SP performs attr transformations
SP performs attr filtering
SP stores transformed attrs
SP redirects to original url; sets session cookie

SP looks up attr info based on cookie and stored info
SP sets environment variables for App

(browser)

Legend: Flows in parens () are the second half of a redirect

(AuthN response w/ attrs)

(Redirect to http://example.com/App; session cookie sent)