Shibboleth & DLT

Mark Earnest
Emerging Technologies

What is Shibboleth

- Federated Authentication & Authorization
- Emphasis on protection of privacy
- Builds on eduPerson, SAML, and PKI to provide secure exchange of interoperable attributes

eduPerson

- Internet2/Educause initiative
- LDAP object class to describe individuals in higher education
- Agreed upon schema and values allow for inter-realm authorization decisions

SAML

- Security Assertion Markup Language
- A way to represent authentication and attributes in XML
- Integrity and trust ensured by cryptographically signing the XML assertion

Shibboleth Goals

- Authentication / Attribute store agnostic
- Platform and web server agnostic
- Utilize existing open standards
- Provide mechanism to protect privacy

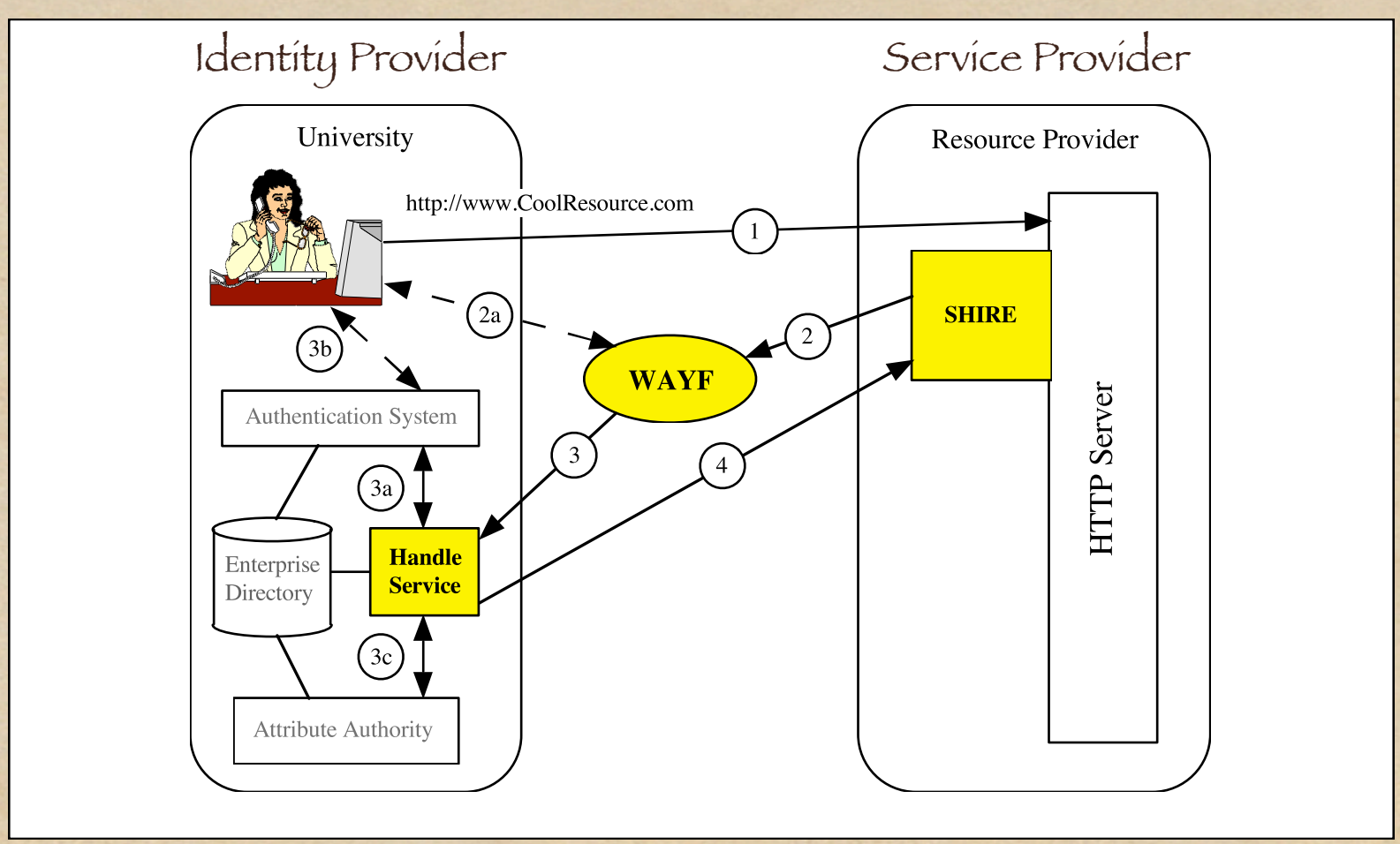
Identity Provider

- Ties in with existing authn/authz systems
- Generates SAML assertions
- Allows fine grained control over attribute release

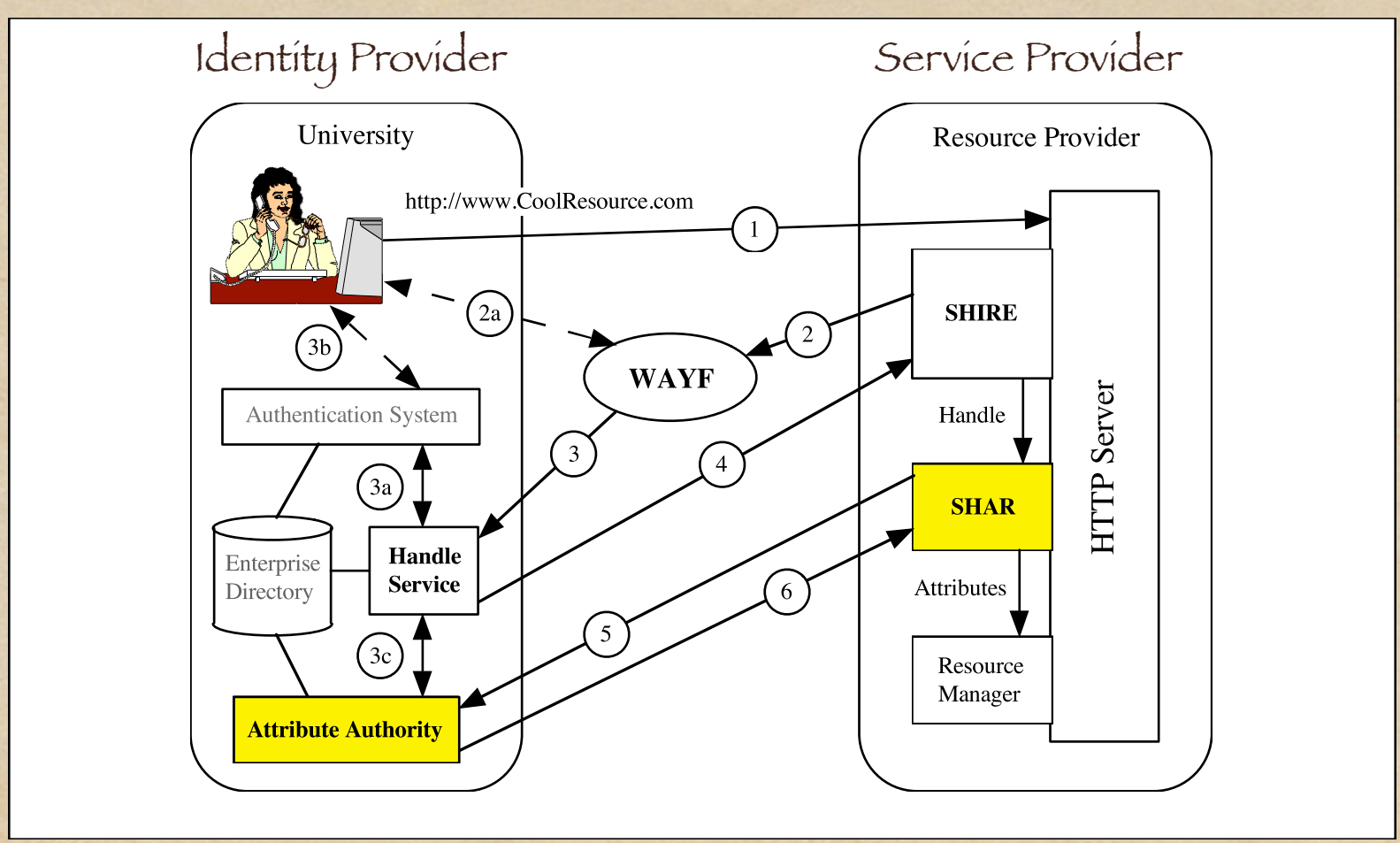
Service Provider

- Runs as a web server module & daemon
- Receives SAML assertions from Identity Provider
- Provides web application with user attributes in the form of environment variables

Authentication



Authorization



Federations

- Associations of enterprises that agree to share information about users and resources
- Provides consistency in inter-realm policy, attributes, and trust.
- Attribute release policies can be delegated to the federation

Digital Repositories

- EBSCO - production
- Jstor - testing
- OCLC - testing/pilot
- Proquest - pilot

EZproxy Plans

- Webaccess enable EXprozy (summer '05)
- Webaccess enable PSU's Identity Provider (summer '05)
- This will allow for a seamless, single sign on experience to all library resources

Obligatory Final Slide

- Thank you
- Questions? Discussion?
- mxe20@psu.edu