Shibboleth Architecture
Protocols and Profiles

Corban Rivera
Motivation

♦ web single sign-on and attribute exchange mechanism

♦ Federalized identity authentication mechanism
Single Sign-On (SSO)

1. User Agent attempts to access some resource at the Service Provider

2. Shibboleth Authentication Request issued by Service Provider to WAYF Service or Identity Provider

3. If WAYF used, then User Agent selects Identity Provider, to which Authentication Request is forwarded

4. Identity Provider identifies Principal (methods vary, details not shown)

5. `<saml:Response>` message issued by Identity Provider to Service Provider, and MAY contain SAML attributes

6. Service Provider sends `<saml:AttributeQuery>` to Identity Provider

7. Identity Provider returns `<saml:Assertion>` to Service Provider

8. Based on the Identity Provider’s assertion(s) identifying the Principal, the Service Provider either returns the resource or an (HTTP) error
Authentication Request Profile

♦ When requesting a secured resource
  – Redirect to authentication service
  – Encode using GET method
    • providerId=IP,
    • shire=Service Provider,
    • target=Secured Resource
  – <samlp:Request> queries attributes from IP
Where are you from? (WAYF)

- Used to discover the IP of the requester
- Redirects authentication requests to the requesters IP
Authentication Response Profiles

- **Browser/POST**
  - Message format:
    - providerId=IP,
      shire=action,
      target=target
  - IP returns error, or forwards to Inter-site Transfer Service
  - `<samlp:Response>` sends attributes

- **Browser/Artifact**
  - Message format:
    - SAMLart=artifactid,
      target=target
  - IP returns error, or forwards to Artifact Resolution Service
  - `<samlp:Response>` sends attributes