Account Linking for the Grid

Isaac Potoczny-Jones | Josh Hoyt | OSG All Hands Meeting | 7 March 2011

Talk Roadmap

- Who: A little bit about us
- Why: A discussion of the problem we’re solving
- How: Some details about the solution

Themes

Collaboration

Enabling collaboration is our ultimate goal

Digital Identity

Identity management is a barrier to collaboration

Security

Identity management is a security problem

| galois |

Who We Are

About Galois: Trustworthiness in Critical Systems

Founded in 1999

35 full-time employees

Based in Portland, Oregon

How we like to work

Collaboration

Working together to solve complex problems

Open Innovation

Good ideas should cross organizational boundaries

Open Source

Supporting communities for long-term value

Key contributors

Isaac Potoczny-Jones

- Secure collaboration specialist
- Leader of Galois' Assured Information Sharing program

Josh Hoyt

- Identity management specialist
- Including commercial web development of ID systems
- Editor of the OpenID 2.0 specification

Technical advisory group

- Mine Altunay (OSG)
- Ian Stokes-Rees (SBGrid/NEBioGrid)
- John Hover (ATLAS)
- Burt Holzman (CMS)

Thank you!

Galois' Account Linking Effort

- Funded by DOE's SBIR program
  - Moving innovations into practice
- 2-year project, ending July 2012

Focus: Bring modern collaboration tools to scientists who depend on grid computing

The Problem We’re Solving

Need

Consistently grant access privileges across software using different identity management systems, regardless of how the user authenticates or identifies themselves.

Use Case

- Josh clicks on a link to analysis results that Isaac posted
- The data is accessible only to VO members
- Josh’s certificate is not loaded into his browser

Problem

No current capability exists to link equivalent subject identifiers between systems, so software cannot grant appropriate privileges to users.

Use Case

- Josh identifies himself as `j3h@GALOIS.COM`
- Server knows `CN=Josh Hoyt 36333` is a VO member
- The server can't grant access because it does not know:

```
j3h@GALOIS.COM === CN=Josh Hoyt 36333
```

Core problem: multiple identities

- We all deal with managing multiple identity systems
- *Identity federation* is the leading solution
  - Standards: GSI, SAML, OpenID, OAuth, WS-Federation, …
  - Technologies: Globus, Shibboleth, Facebook Connect, …
- This is not a green field

Why Grid users have multiple identities

Grid VOs:

- Different organizations have different identity systems
- Interfacing with external service providers (the grid!)
- Users need to collaborate across org. boundaries

Why aren’t certificates the whole solution?

- Secure certificate management is complicated
  - Export/import
  - Format conversion
  - Another password
- The Internet is not moving toward certificate federation
- Many applications & collaboration tools don’t support them

Solution Approach

Solution

Develop an system to link subject identifiers between identity management systems:

- *Abstract Program Interface (API)*
- *Set of management tools*
- *An integration plan*

Use Case

- The Web server can consult the Account Linking service to determine that `j3h@GALOIS.COM` and `CN=Josh Hoyt 36333` are equivalent
- The Web server grants access to Josh

Solution goals

- Removes a barrier to collaboration
- Applicable in the long term
- Tractable in the short term
- Fits in to a variety of environments
  - Approach not bound to a particular protocol or software
  - Easy to integrate
- Easy for the end users

Approach benefits

- Using identity information across boundaries
- Requires minimal cooperation from IdPs and applications
- Allows users to authenticate to Web applications in the most appropriate way
- Agnostic to federation protocol (SAML, OpenID, WS-Fed)

Prototype plans

- Build a prototype over the next few months
- Should be easy to understand, set up, and maintain
- We want to do test integration with multiple VOs
- See you back here next year to report on solution?

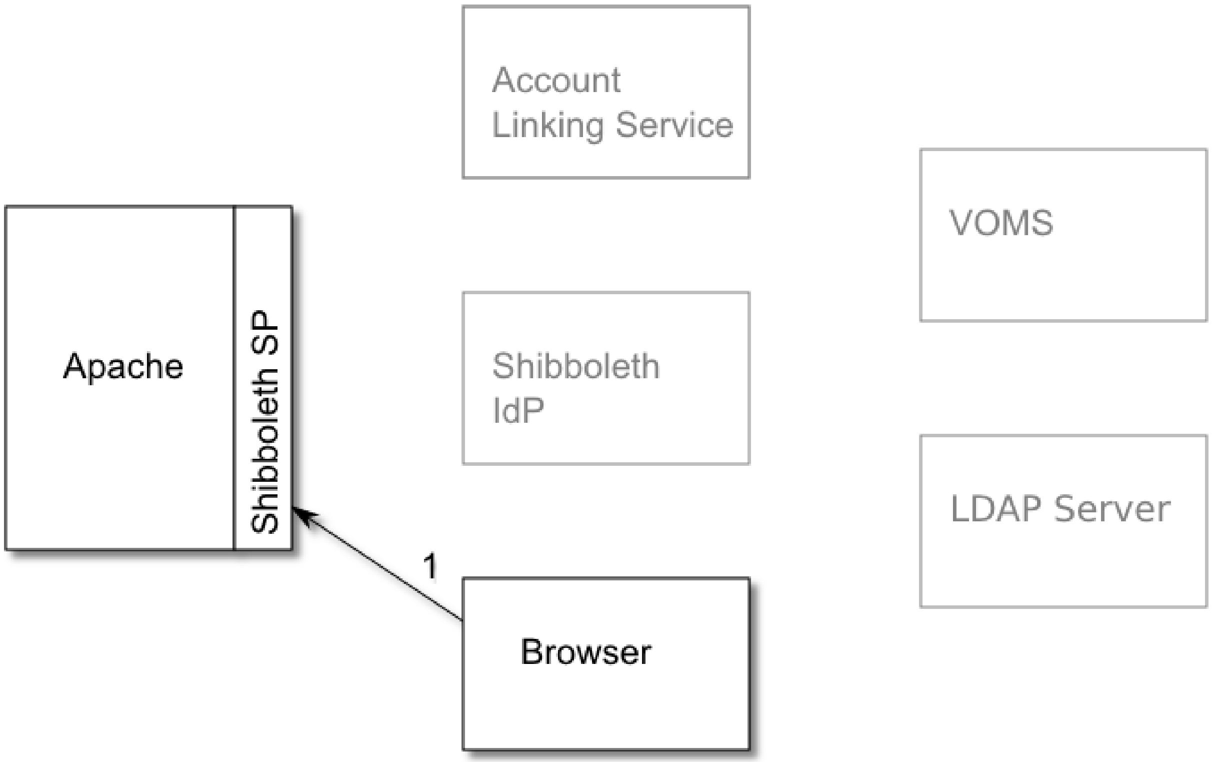
Thank you

- We welcome feedback
- Ask us questions

- http://grid2.galois.com/
- Josh Hoyt <josh.hoyt@galois.com>
- Isaac Potoczny-Jones <ijones@galois.com>

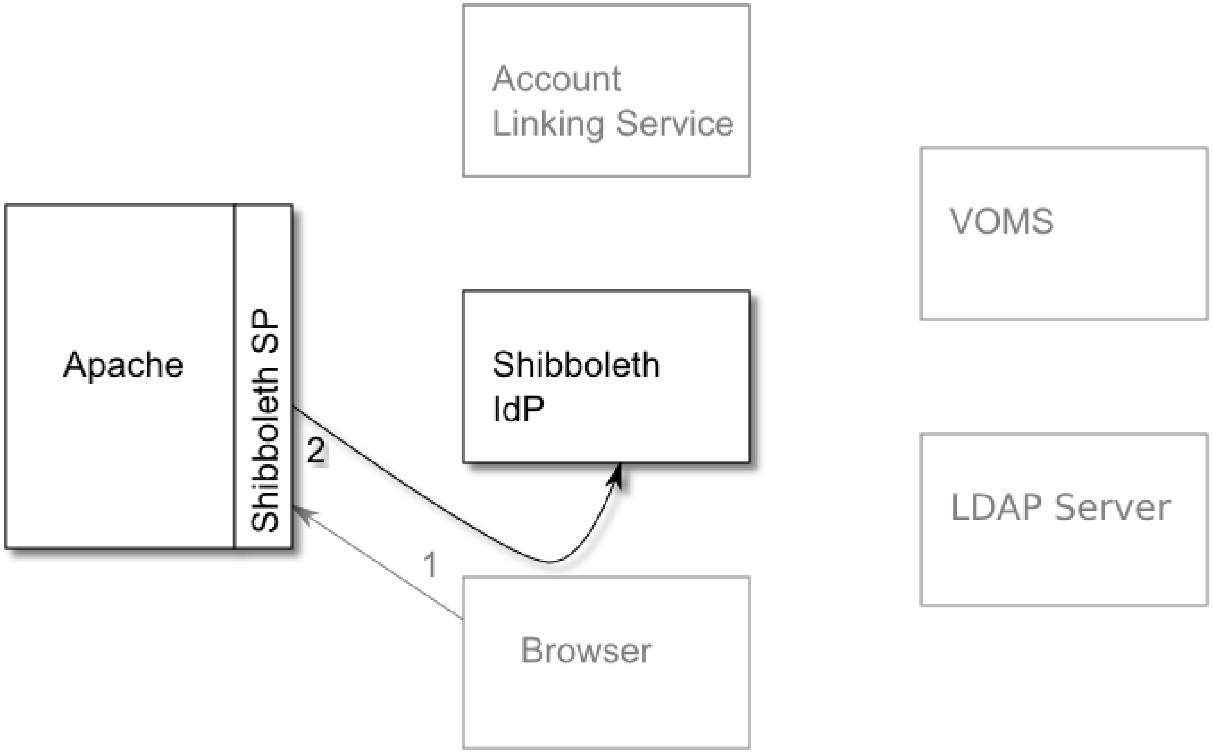
BACK-UP SLIDES

Use case walk through: 1



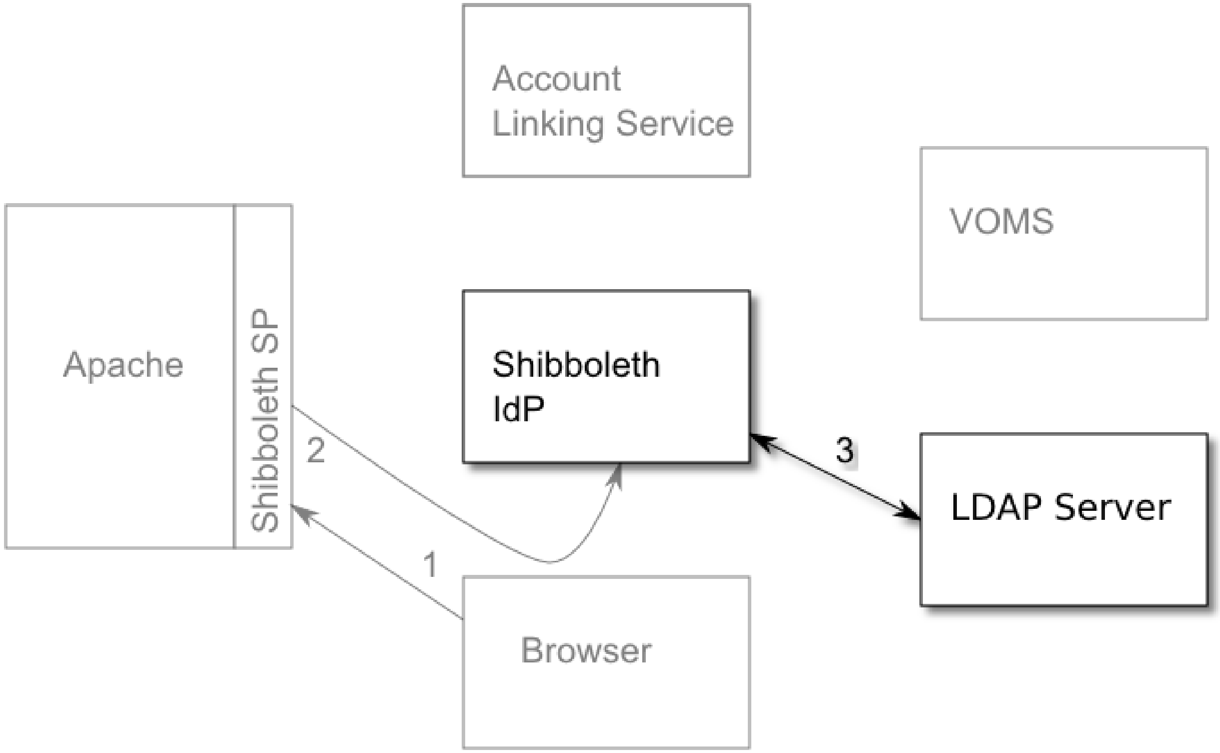
The user clicks on a link handled by Apache

Use case walk through: 2



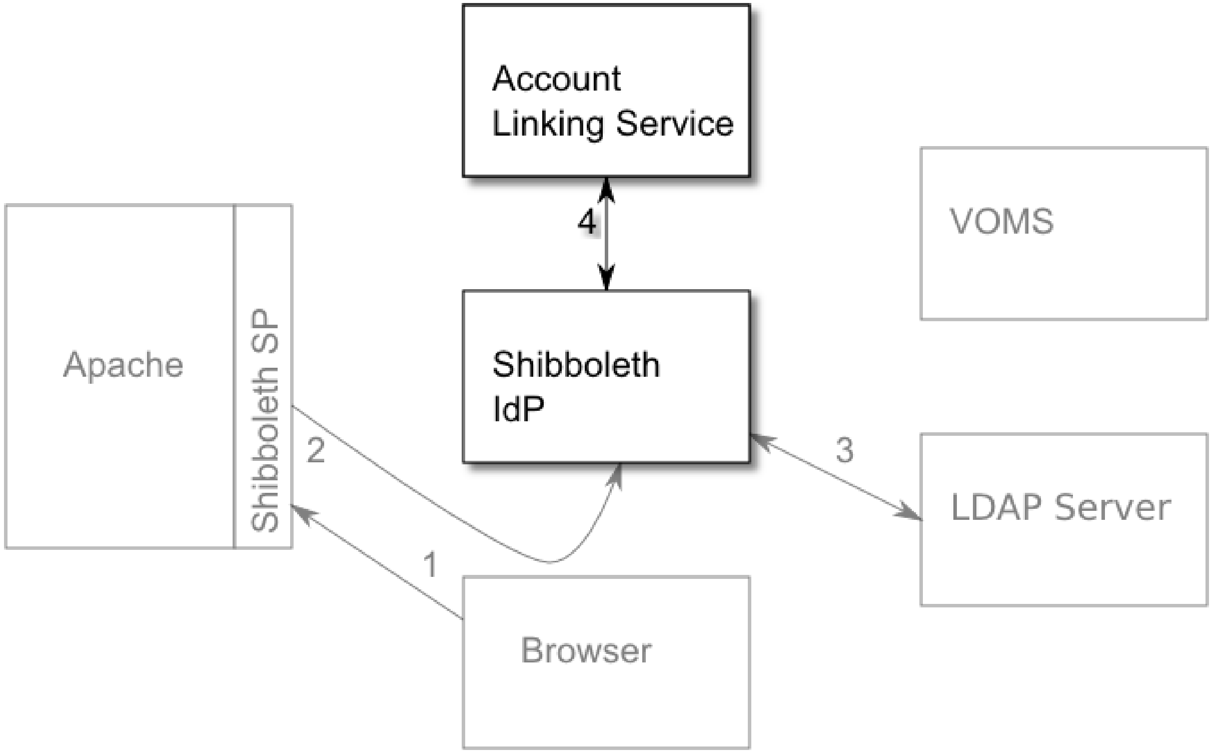
Apache redirects the user to the IdP

Use case walk through: 3



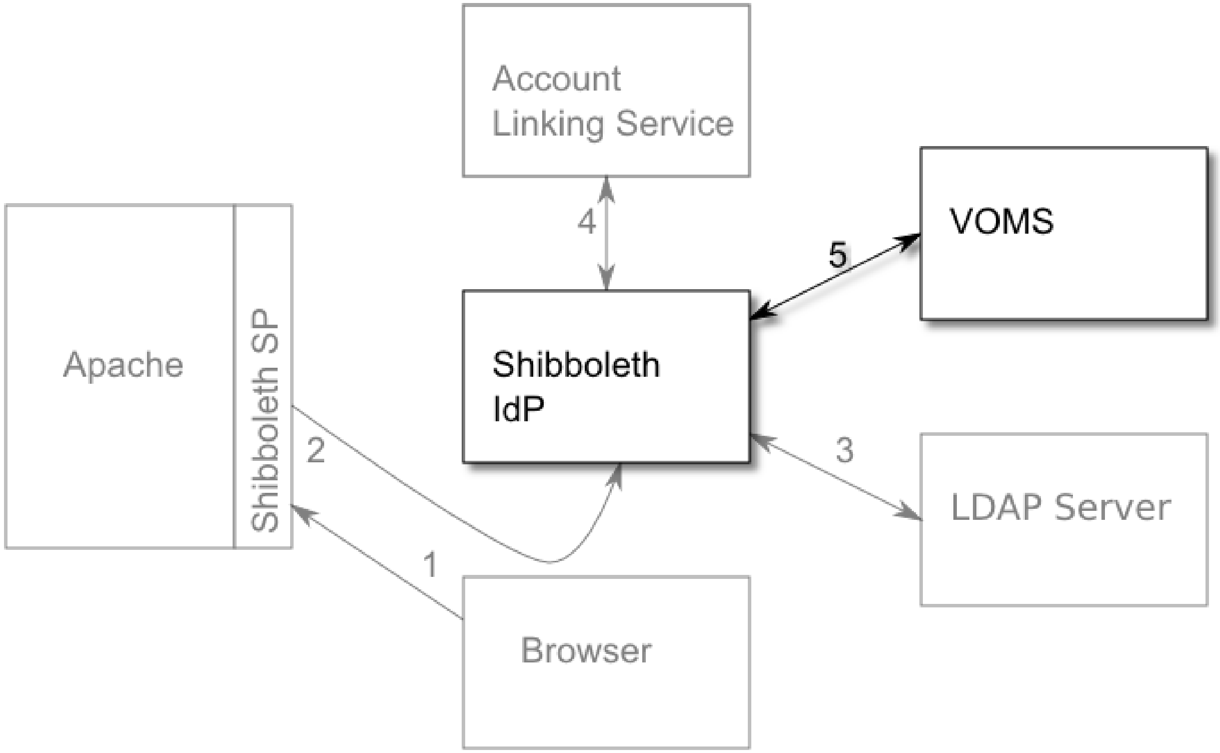
The IdP requests user information from the LDAP server

Use case walk through: 4



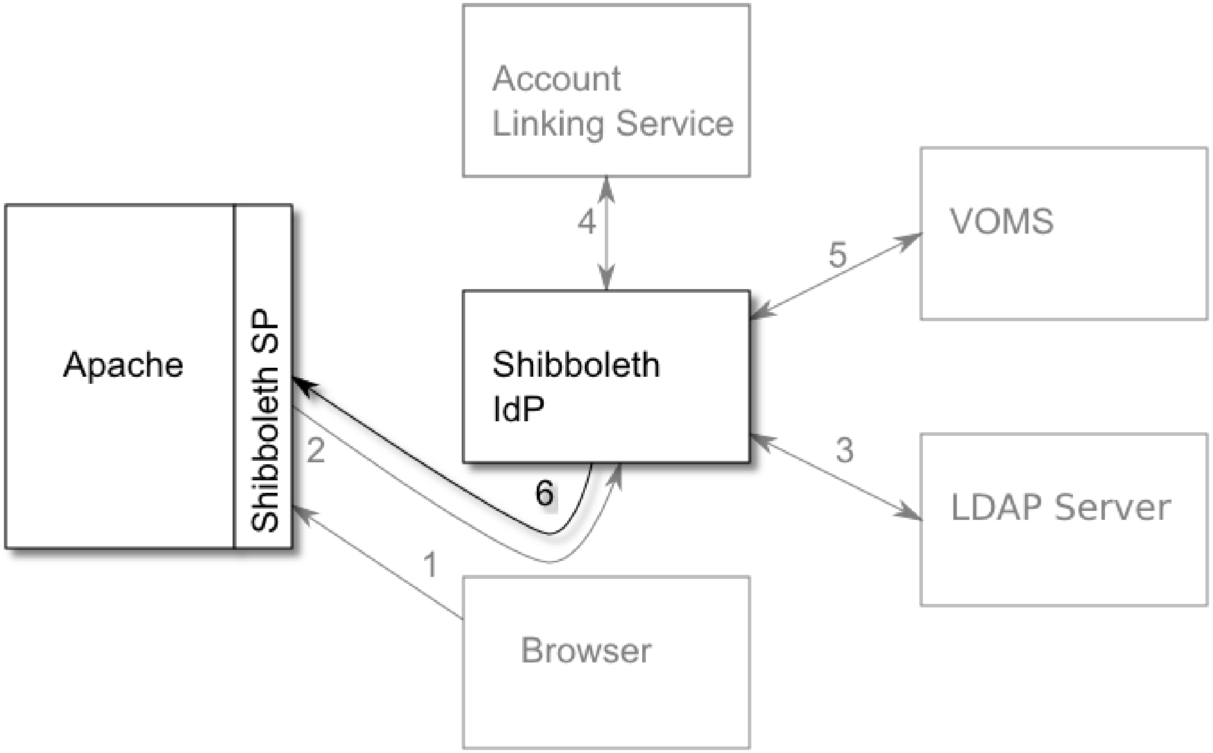
The IdP uses the Account Linking Service to get the user’s DN

Use case walk through: 5



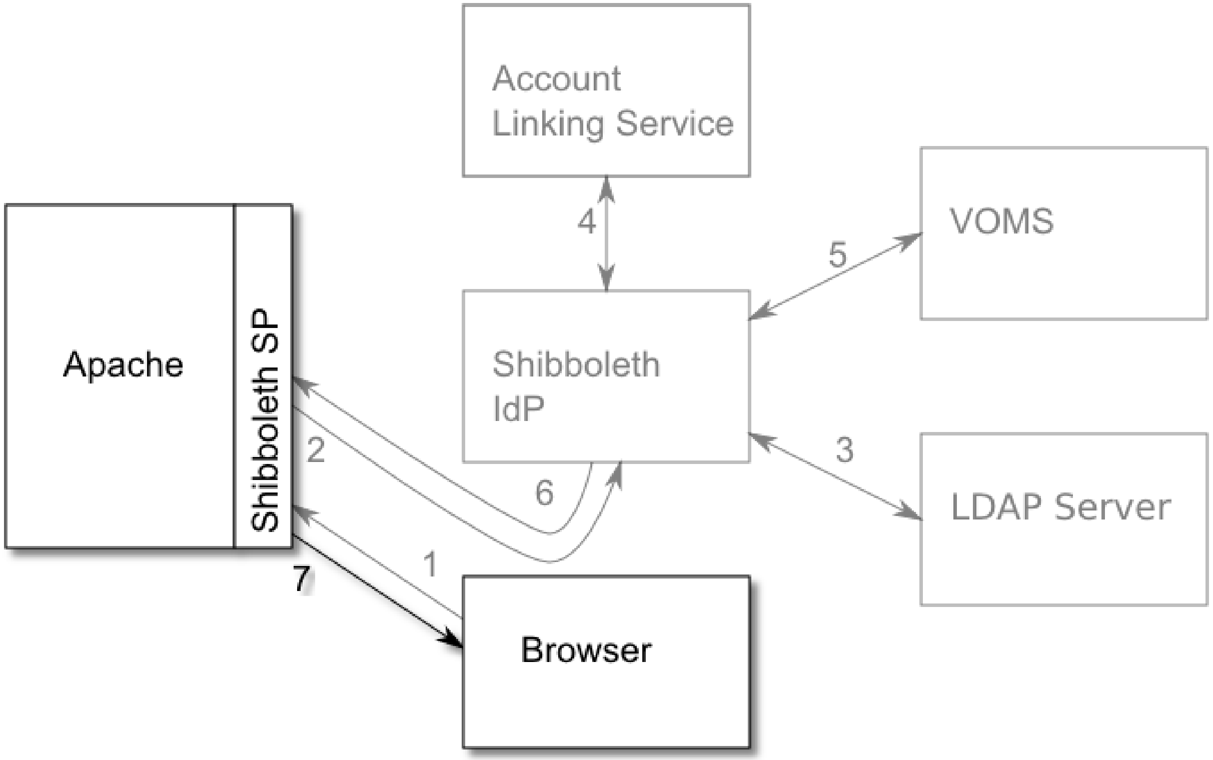
The IdP requests group information from VOMS using the DN

Use case walk through: 6



The IdP redirects the user back to Apache with the LDAP and VOMS attributes

Use case walk through: 7



Apache serves the user’s original request