Introduction to Shibboleth

Daniel Lutz
aai@switch.ch

SWITCHaai Introduction Course
Bern, 1. March 2013

Agenda

- What is Shibboleth?
- IdP/SP Communication
- Shibboleth
- Support Resources

Shibboleth – Origin and Consortium

- The Origin
  - Internet2 in the US launched the open source project
- The name
  - Word **Shibboleth** was used to identify members of a group
- The standard
  - Based on Security Assertion Markup Language (SAML)
- The Consortium
  - The new home for Shibboleth development
  - collect financial contributions from deployers worldwide

http://shibboleth.net

What is Shibboleth? (1)

- Technically it’s a project group, like Apache or Eclipse, whose core team maintains a set of software components
- Most people think of it as the set of software components
  - OpenSAML C++ and Java libraries
  - Shibboleth Identity Provider (IdP)
  - Shibboleth Service Provider (SP)
  - Shibboleth Discovery Service (DS)
  - Shibboleth Metadata Aggregator (MA)
- Taken together these components make up a federated identity management (FIM) platform.
- You might also think of Shibboleth as a multi-protocol platform that enforces a consistent set of policies.

What is Shibboleth? (2)

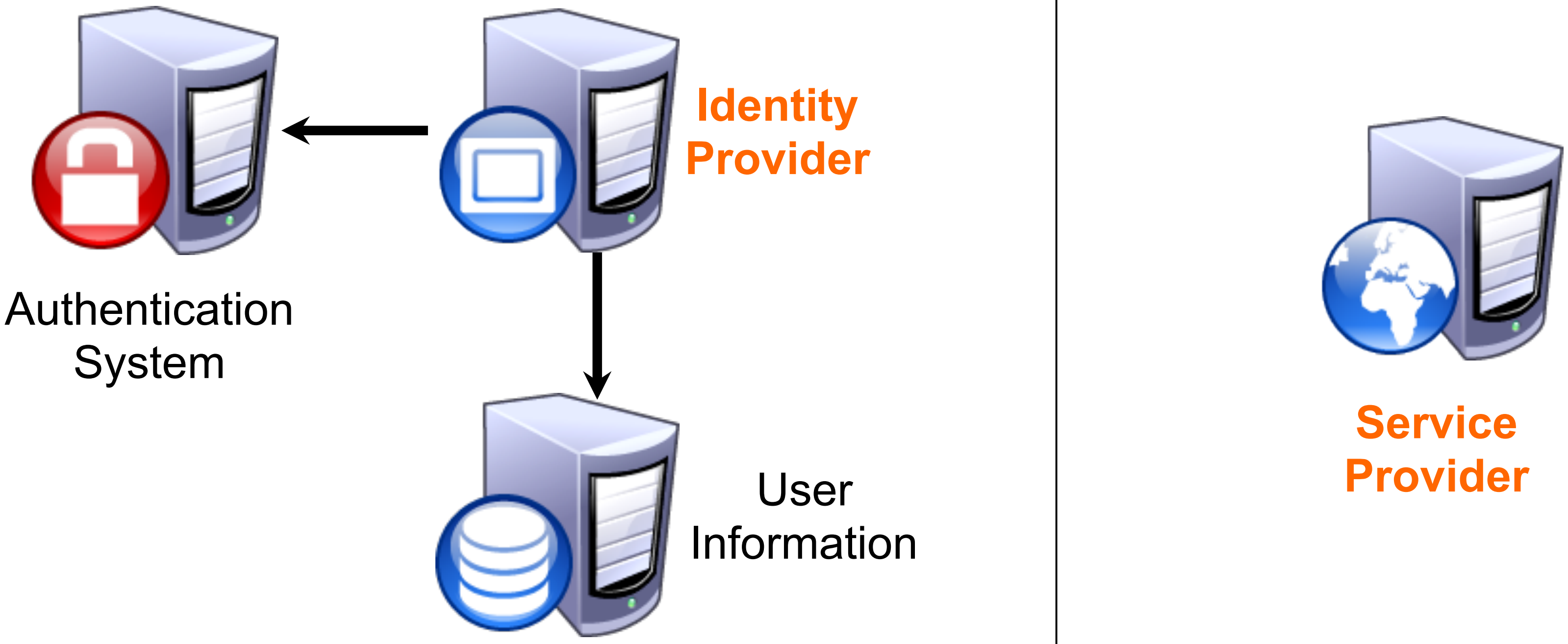
- The Shibboleth software components are an implementation of the SAML protocols and bindings. There are other products, too (like e.g. SimpleSAMLphp).

- The Shibboleth software is widely used in the research and education environment

The Components

@ home organization

@service organization



Authentication System

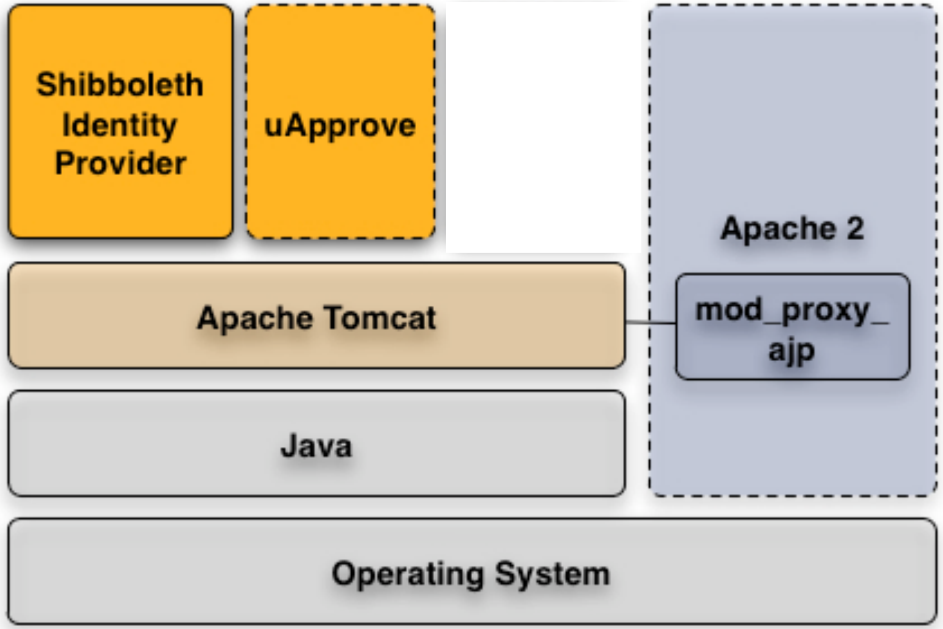
Identity Provider

User Information

Service Provider

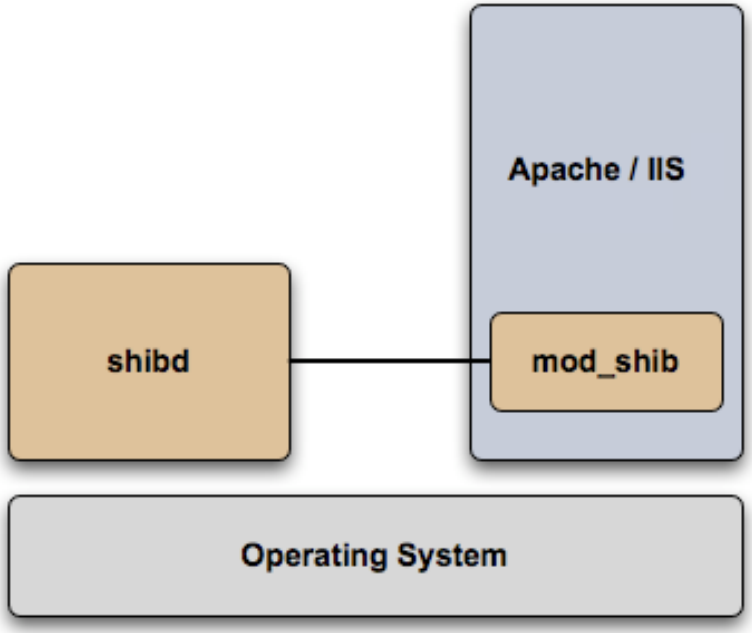
Shibboleth Components: Identity Provider

- What is it?
  - A Java Servlet (2.4) web application
- What does it do?
  - Connects to **existing** authentication and user data systems
  - Provides information about how a user has been authenticated
  - Provides user identity information from the data source



Shibboleth Components: Service Provider

- What is it?
  - mod_shib: A C++ web server (Apache/IIS) module
  - shibd: A C++ daemon - keeps state when web server processes die
- What does it do?
  - Optionally initiates the request for authentication and attributes
  - Processes incoming authentication and attribute information
  - Optionally evaluates content access control rules



Terminology (1)

- SAML - Security Assertion Markup Language
  The standard describing the XML messages sent back and forth by the Shibboleth components (two versions: 1.1, 2.0)

- Profile - Standard describing how to use SAML to accomplish a specific task (e.g. SSO, attribute query)

- Binding - Standard that describes how to take a profile message and send it over a specific transport (e.g. HTTP)

Terminology (2)

- entityID - Unique identifier for an IdP or SP
- NameID - An identifier by which an IdP knows a user
- Attribute - A named piece of information about a user
- Assertion - The unit of information in SAML

Shibboleth Supported Profiles

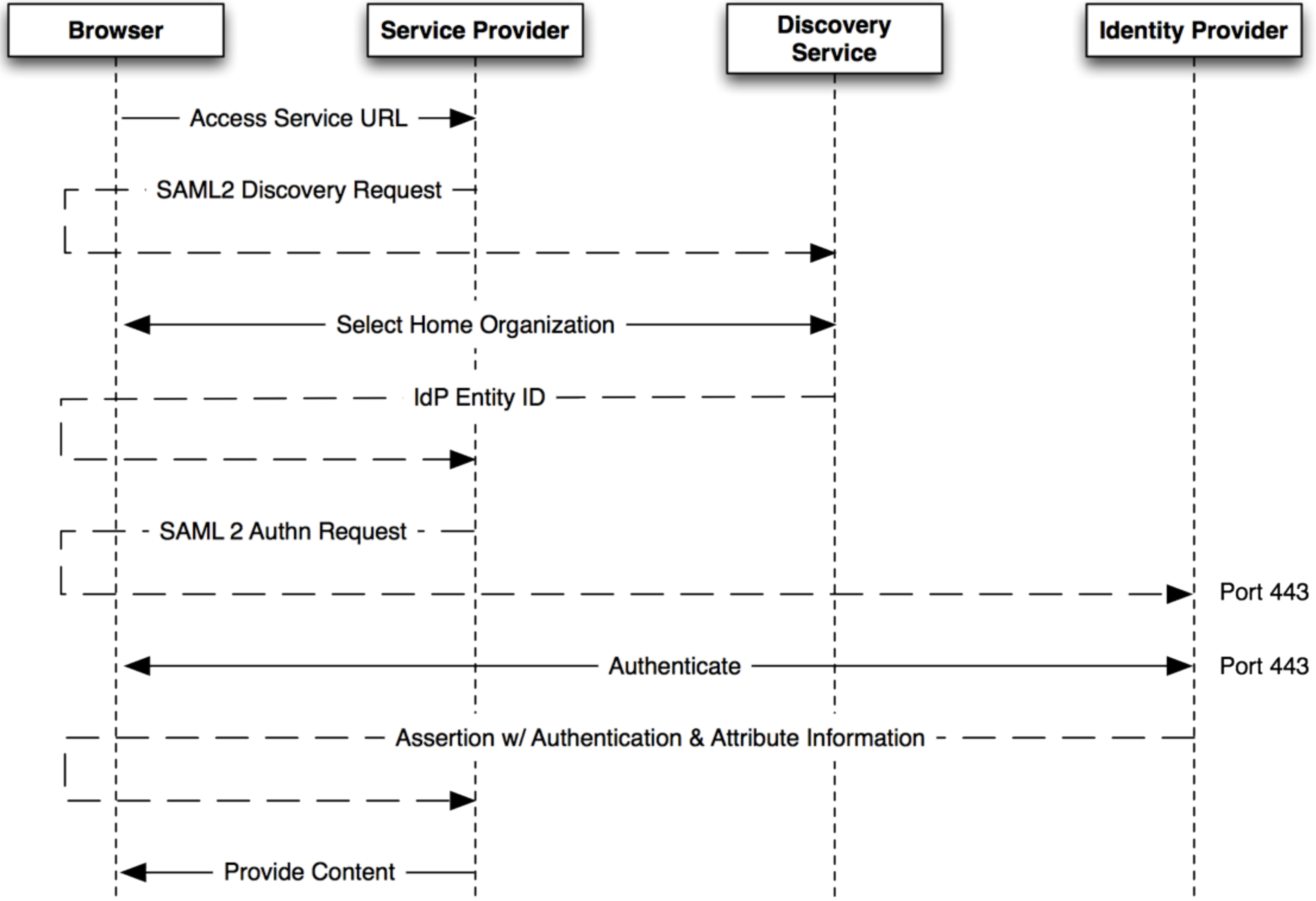
- SAML 2
  - SSO
  - Attribute Query
  - Artifact Resolution
  - Enhanced Client
  - Single Logout (SP-only)

- SAML 1 (deprecated)
  - Shibboleth SSO
  - Attribute Query
  - Artifact Resolution

- Discovery
  - SAML 2 Discovery Service (not used in SWITCHaai)
  - Shibboleth 1 Discovery (WAYF) (deprecated; not used in SWTICHaai)

https://wiki.shibboleth.net/confluence/display/DEV/Supported+Protocols

Shibboleth Communication Flow: Shibboleth 2 SSO



Odds and Ends

- Shibboleth knows nothing about federations, it just consumes metadata in order to:
  - locate the entity to which messages are sent
  - determine what protocols the entity supports
  - determine what signing/encryption keys to use

- The IdP is CPU bound, unlike most web apps
  - No support for crypto-acceleration currently
  - Limited support for clustering though

Support Resources

- First, check with your Federation
  - http://switch.ch/aai/support/documents
  - http://switch.ch/aai/support/help
- Shibboleth Wiki
  - https://wiki.shibboleth.net/confluence/display/SHIB2
- Shibboleth Mailing Lists
  - Available lists: http://shibboleth.net/community/lists.html
    - Users
    - Announcements
    - Development
  - User's list archive: http://marc.info/?l=shibboleth-users