Introduction to Shibboleth

SWITCH
Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

Agenda

- What is Shibboleth?
- IdP/SP Communication
- Shibboleth 1 & 2
- 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

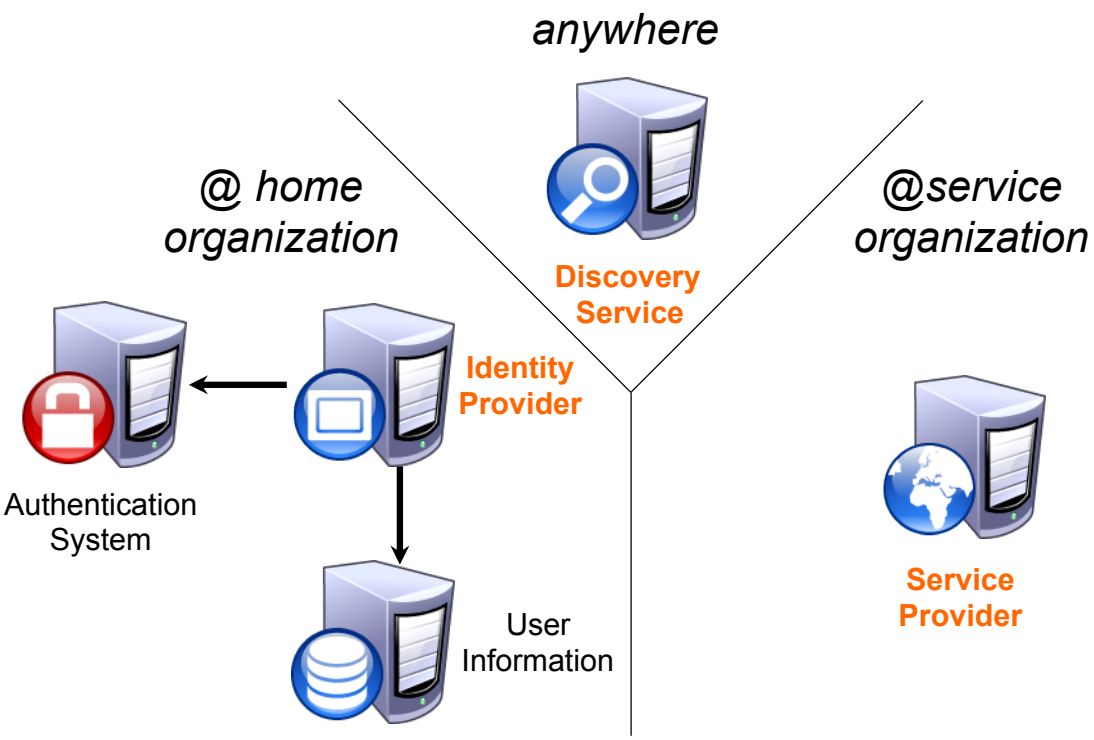
http://shibboleth.net

What is Shibboleth?

- 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)

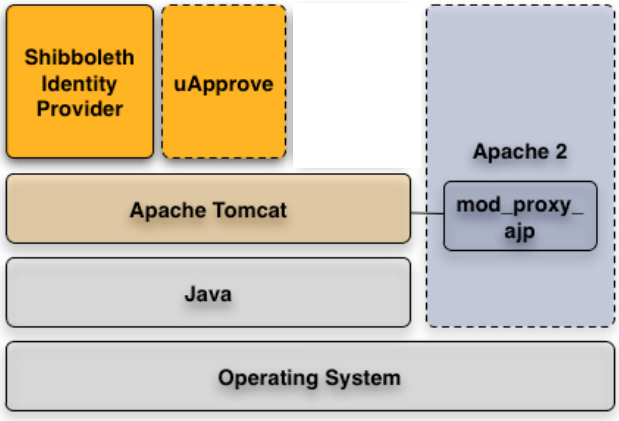
- Taken together these components make up a federated identity management (FIM) platform.
- You might also think of Shibboleth as a multi-protocol platform that enforces a consistent set of policies.

The Components



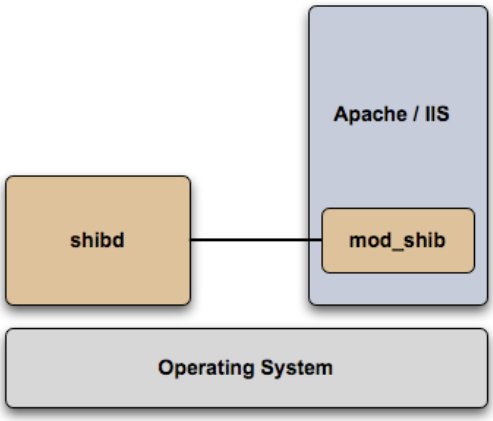
Shibboleth Components: Identity Provider

- 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



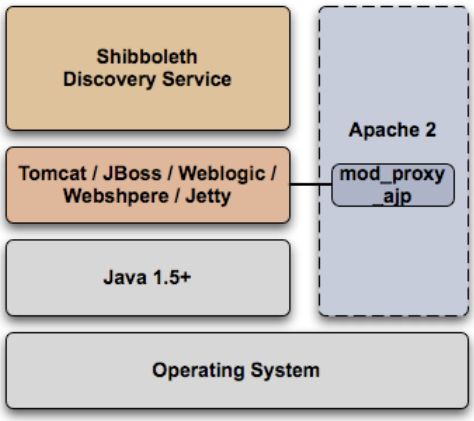
Shibboleth Components: Service Provider

- 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



Shibboleth Components: Discovery Service

- What is it?
  - A Java Servlet (2.4) web application
- What does it do?
  - Asks the user to select their home organization from a list



See also an Alternative Implementation: http://switch.ch/aai/wayf

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)
- Front-channel - A binding that sends message through a user's browser via redirects or form posts
- Back-channel - A binding where the entities connect directly to each other

Terminology (2)

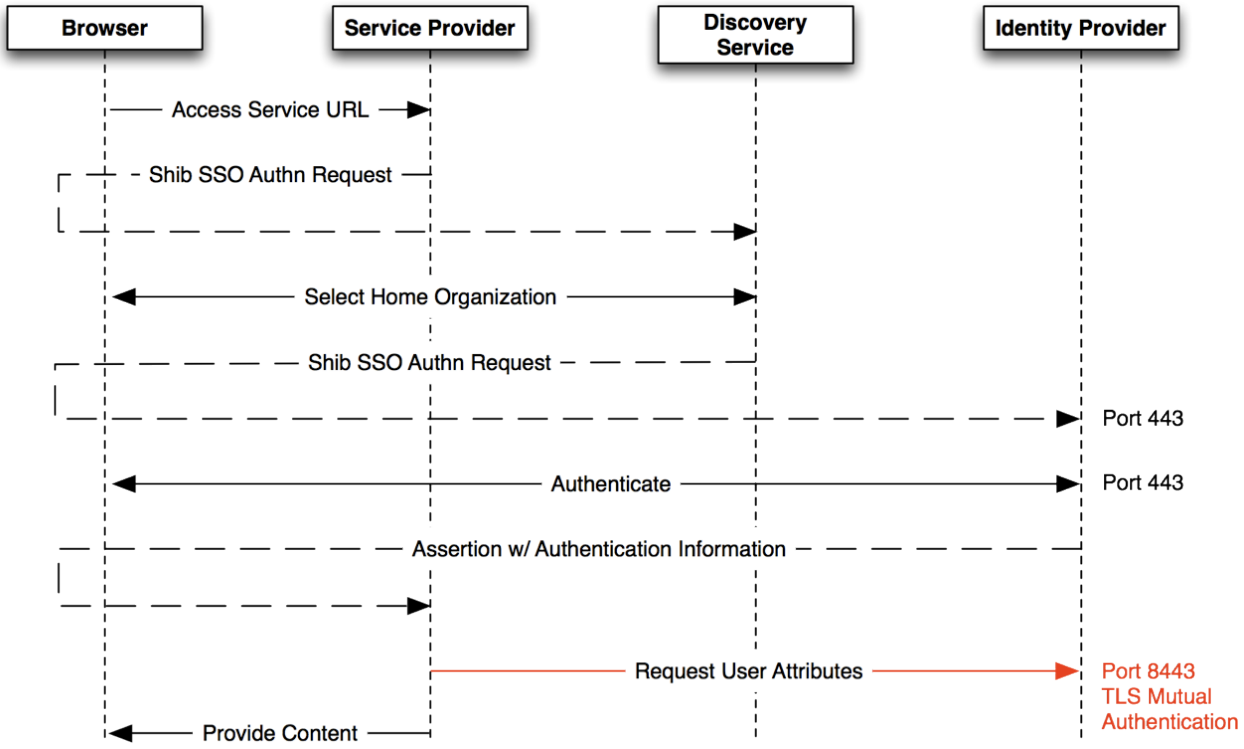
- entityID - Unique identifier for an IdP or SP
- Assertion - The unit of information in SAML
- NameID - An identifier by which an IdP knows a user
- Attribute - A named piece of information about a user

Shibboleth Supported Profiles

- SAML 1
  - Shibboleth SSO
  - Attribute Query
  - Artifact Resolution
- SAML 2
  - SSO
  - Attribute Query
  - Artifact Resolution
  - Enhanced Client
  - Single Logout (SP-only)
- Discovery
  - Shibboleth 1 Discovery (WAYF)
  - SAML 2 Discovery Service

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

Shibboleth Communication Flow: Shibboleth 1

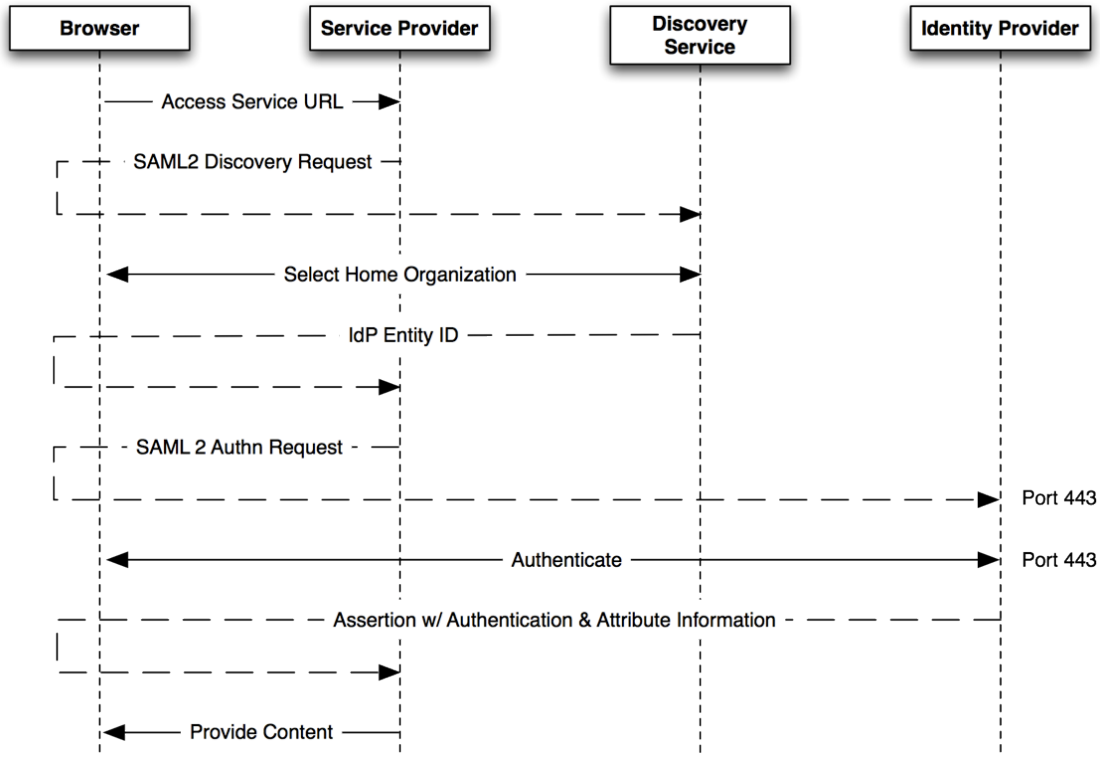


Problems with Shibboleth 1 SSO Flow

- The SP does not know which IdP will receive its request and so it can not tailor the authentication request
  - Which protocol to use?
  - Which keys to use for encryption?

- The IdP must have a second SSL port in order for the SP to make its attribute query (attribute pull model)
  - Twice the number of crypto operations
  - Two request/response pairs for every authentication

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
  - Support for clustering though

Shibboleth 1.3 to 2.X migration

- Shibboleth 2 is backwards compatible with 1.3
  - Obviously new SAML 2 features don't work with Shibboleth 1.3
- Entity's should embed their certificates in their metadata
  - This is required in order to support SAML 2 encryption
- The Shibboleth team recommends URLs for entityIDs
  - IdP entityID: **`https://HOSTNAME/idp/shibboleth`**
  - SP entityID: **`https://HOSTNAME/shibboleth`**
  - These URLs can then be used to get the metadata for the entity

SP Migration: Attribute Names

- Version 1.3 placed attributes in HTTP Headers

```
HTTP_SHIB_EP_AFFILIATION              staff
HTTP_SHIB_INETORGPERSON_GIVENNAME     Lukas
```

- Version 2.0 (when using Apache) places attributes in server environment and uses slightly different names as a result

```
Shib-EP-Affiliation                 staff
Shib-InetOrgePerson-givenName       Lukas
```

- Version 2.0 supports the old method but the new method guarantees that information can not be spoofed

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 User's Mailing List Archive
  - http://marc.info/?l=shibboleth-users
- Shibboleth User's Mailing List
  - http://shibboleth.net/community/lists.html