Introduction to Shibboleth

SWITCHaai Team
aai@switch.ch

Agenda

- What is Shibboleth?
- Components
- Supported Profiles and Protocols
- Shibboleth in the Federation
- Support Resources

Shibboleth – Origin and Consortium

- The Origin
  - Internet2 in the US launched the open source project in 2000
- 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)

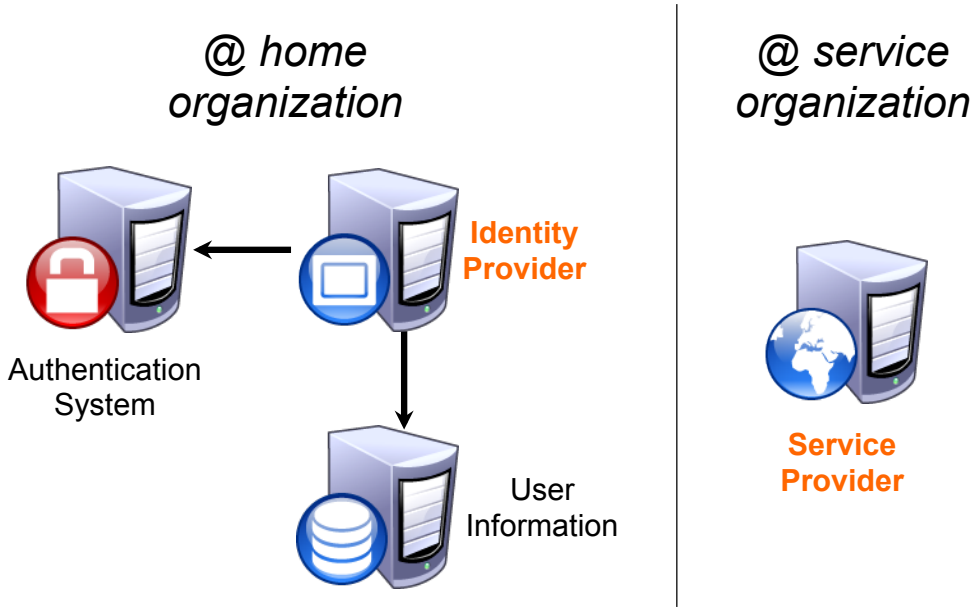
- Technically it's a project group, like Apache or Eclipse, whose core team maintains a set of software components
- Most people think of it as the set of software components
  - OpenSAML C++ and Java libraries
  - Shibboleth Identity Provider (IdP)
  - Shibboleth Service Provider (SP)
  - Shibboleth 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)

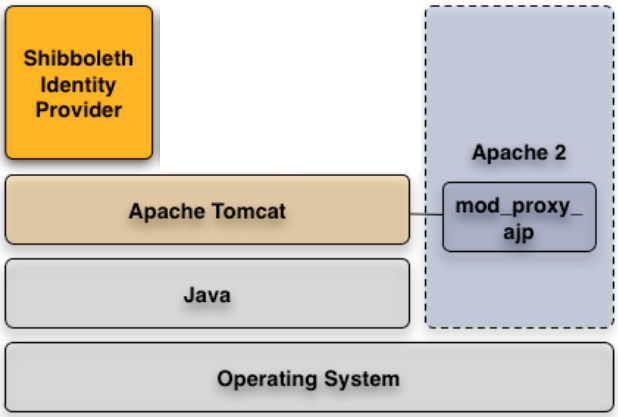
- The Shibboleth software components are an implementation of the SAML protocols and bindings. There are other products, too (like e.g. SimpleSAMLphp, ADFS).
- The Shibboleth software is widely used in the research and education environment

Components used in the SWITCHaai federation



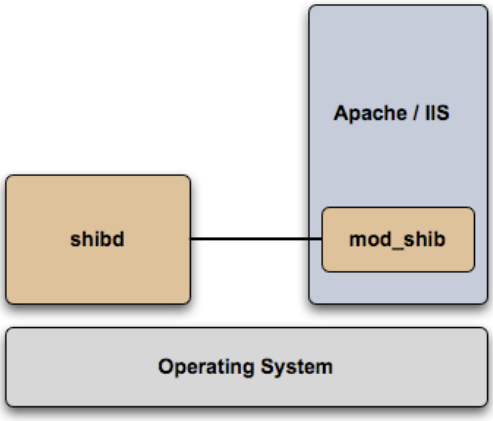
Shibboleth Components: Identity Provider (IdP)

- What is it?
  - A Java Servlet 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 (SP)

- 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?
  - Typically initiates the request for authentication and attributes
  - Processes incoming authentication and attribute information
  - Optionally evaluates content access control rules



Shibboleth Components: Others

Further Shibboleth components:

- Shibboleth Discovery Service (DS)
  - Not used in SWITCHaai
  - Instead, we use the SWITCHaai WAYF
- Shibboleth Metadata Aggregator (MA)
  - Used in the Resource Registry to support Interfederation resources

Shibboleth Supported Profiles and Protocols

- SAML 2.0
  - **SSO**
  - Attribute Query
  - Artifact Resolution
  - Enhanced Client
  - Single Logout (SP-only)
- SAML 1.1 (deprecated)
  - SSO Profile
  - Shibboleth SSO Request Profile
  - Attribute Query
  - Artifact Resolution
- Discovery
  - **SAML 2 Discovery Service Protocol**
  - Shibboleth 1 Discovery (WAYF) Protocol

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

Shibboleth in the Federation

- 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 “Resource Registry”, a central registry in the SWITCHaai federation, generates the metadata and makes all IdPs and SPs know each other
  - The Resource Registry knows all IdPs, SPs, supported protocols, service locations and signing/encryption keys

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
  - https://wiki.shibboleth.net/confluence/display/IDP30
- Shibboleth Mailing Lists
  - Available lists: http://shibboleth.net/community/lists.html
    - Users
    - Announcements
    - Development
  - User's list archive: http://marc.info/?l=shibboleth-users