Shibboleth

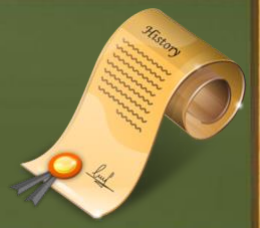
Muhammad **Rizwan** Asghar
The University of Auckland
October 8, 2015

For template of slides,
thanks to kingsoftstore.com

Overview

- Widely used federated identity standard
- Used by educational institutes
- A set of protocols
- Implements SAML
- Free
- Open source

History



- Began as an Internet2 Middleware activity in 2000
- Later (in 2000) the project connected with the work of the OASIS SAML Working Group
- Shibboleth 1.0 was released in 2003
- Shibboleth 2.0 was released in March 2008

Why Shibboleth

- No implementation of identity federation and SSO across domains
- No concept of federated access control

Basic Purpose

- Shibboleth provides cross-domain authorisation
- Focused on preserving privacy of users
- It makes the process of authentication and authorisation scalable

What is Shibboleth

- A middleware architecture for secure exchange of authorisation information
- Authorisation information can be used in making access control decisions

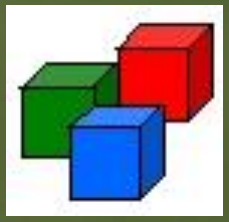
Authorisation Information

- Name
- Attributes
  - Role
  - Group
  - Course membership

In Shibboleth

- A user gets authenticated with her Identity Provider using her credentials
- Identity Providers provide minimal identity information to Service Providers
- Service Providers make authorisation decisions

Main Components



- Identity Provider (IdP)
  - A.k.a. Shibboleth Origin
- Service Provider (SP)
  - A.k.a Shibboleth Target
- Discovery Service
- Both the IdP and the SP must be members of the same federation

Acknowledgements to Nigel Bruce for this and next two slides

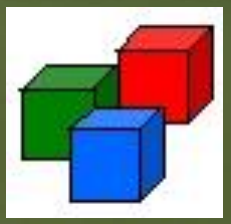
Federation

- A federation is not a technological entity
- It is an agreement between organisations
- Members share a common set of agreed policies and rules in order to establish trust between members

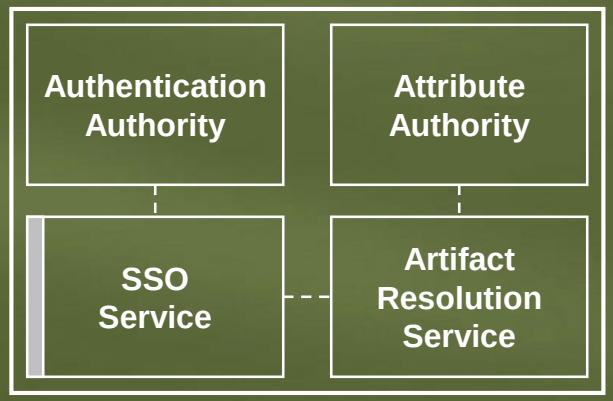
Federation (2)

- Members must ensure
  - Only legitimate users have accounts
  - Accounts are lapsed after people leave
  - Information about users is accurate
  - Acceptable password and security policies

IdP

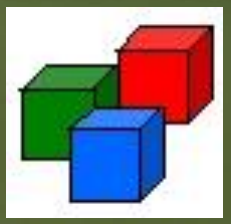


- A Shibboleth IdP creates and manages user identity
- It produces SAML assertions



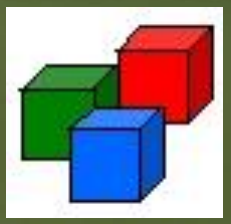
Slide source: Shibboleth: A Technical Overview by Tom Scavo

IdP Sub-Components

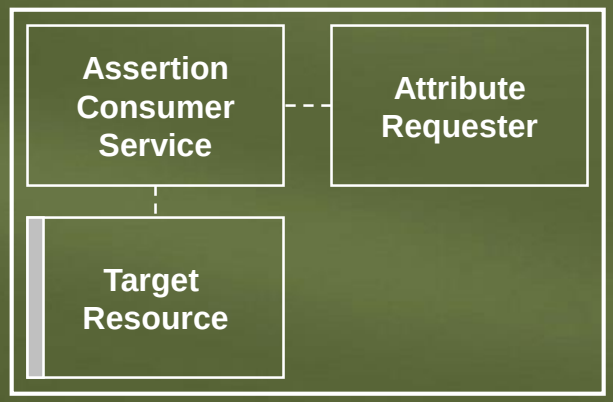


- SSO Service
  - Handles SP-initiated requests
- Authentication Authority
  - Produces SAML authentication assertions
- Attribute Authority
  - Produces SAML attribute assertions
- Artifact Resolution Service
  - Resolves SAML artifacts into assertions

SP

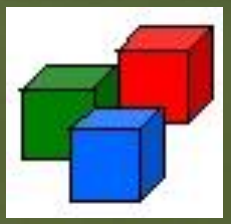


- A Shibboleth SP regulates access to services and resources
- It consumes SAML assertions



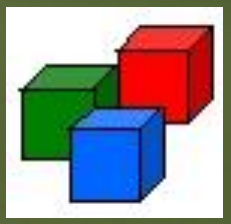
Slide source: Shibboleth: A Technical Overview by Tom Scavo

SP Sub-Components



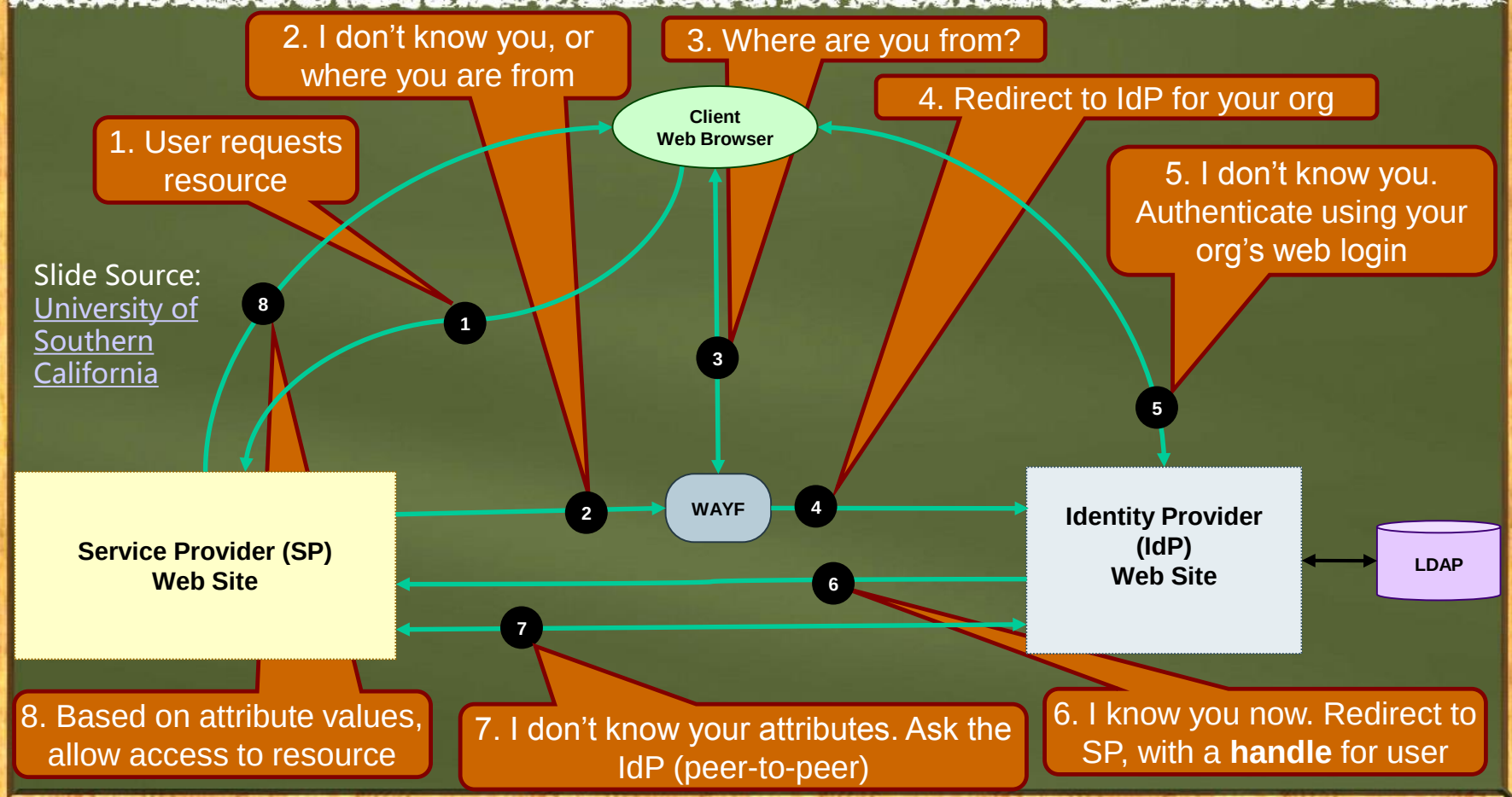
- Assertion Consumer Service
  - Consumes SAML authentication assertions
- Attribute Requester
  - Makes a request to the Attribute Authority at the IdP
  - Consumes SAML attribute assertions
- Target Resource
  - The protected resource that is requested

Discovery Service



- WAYF
  - Where Are You From
- Provides users an interface to choose an IdP
- It is not dependent on IdPs or SPs
- It is optional

Shibboleth Workflow



Shibboleth

- Shibboleth is flexible and does not dictate how authentication should be performed
- Authentication method could be any
  - LDAP
  - Kerberos
  - Certificates
  - …

Shibboleth

- Once authenticated, the IdP generates a pseudonym token called a handle, which is sent to the SP
- The SP uses this handle to request further information about the user
- Based on attribute information received, the SP then makes an authorisation decision

Scenario

- Access to electronic journals
- It does not require complex authorisation decisions
- An assertion that a requester is affiliated to a particular institute is needed

Examples

Research Professional

researchprofessional.com

IEEE

ieeexplore.ieee.org

canvas

learn.canvas.net

And many others ...

Privacy

- Shibboleth is user-centric
- A user controls release of her attributes
  - Who accesses her attributes
  - What attributes are accessed

Security Considerations

- Shibboleth is based on SAML
- For addressing security properties, it can use TLS/SSL as proposed by SAML
  - Exchanged messages can be encrypted
  - Exchanged messages can be signed

Summary

- Shibboleth is widely deployed
- It enables secure information sharing
- It makes authentication and authorisation scalable
- SPs take access control decision based on trusted information provided by IdPs


Q&A

References

- Shibboleth, https://shibboleth.net/
- Shibboleth, http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth/
- Shibboleth Architecture, http://open-systems.ufl.edu/files/draft-mace-shibboleth-tech-overview-latest.pdf

References (2)

- Shibboleth Wiki, https://wiki.shibboleth.net/confluence/display/SHIB2/Home
- Shibboleth: Federated Single Sign-On Authentication Service, http://www.unicon.net/opensource/shibboleth