Shibboleth N-Tier Support

SWITCH

Serving Swiss Universities

Chad La Joie
chad.lajoie@switch.ch

Agenda

- Use Case
- Terminology
- Shibboleth Solution
- Future Effort
- Resources

Use Case

- Current use case comes from University of Chicago
- University uses uPortal which displays information from a set of portlets
- The site hosting each portlet is also a stand-alone, Shibboleth-protected site (i.e. it's an SP)
- Each app displays personalized information based on the user (e.g. number of unread mails, class schedule)

- The goals are:
  - Allow the user to log in to the portal and the portal to log in to the portlets as the user.
  - The SAML assertion given to the portlet should be derived from the SAML assertion given to the portal
  - The SAML assertion given to the portlet should be targeted to the portlet (i.e. filtered identifiers and attributes)

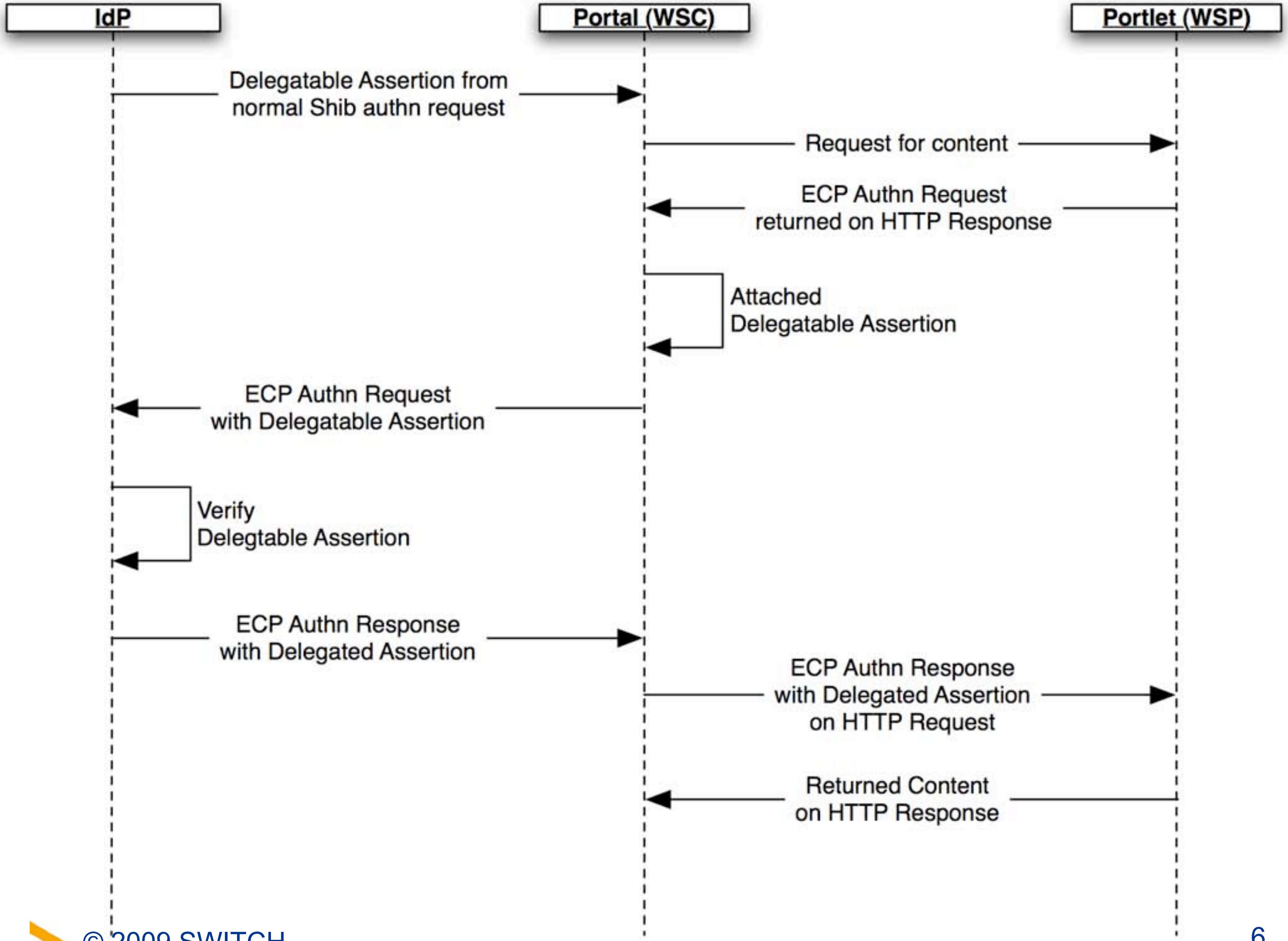
Terminology

- Assertion - A set of statements (e.g. authentication and attributes) by the IdP about a user
- **Delegatable** Assertion - An assertion which may be used to get another assertion targeted for another service.
- **Delegated** Assertion - An assertion derived from a delegatable assertion.
- Delegation - The process of taking a delegatable assertion and turning it in to a delegated assertion.
- Web Service Provider (WSP) - non-browser based, SAML service provider
- Web Service Client (WSC) - client used to request content from the WSP, must offer ECP support
- Enhanced Client/Proxy (ECP) - a SAML binding that does not require, but does allow, the use of a browser

Shibboleth Solution

1. User authenticates to portal with a delegatable assertion
2. Portal attempts to contact portlet which returns an ECP authentication request
3. Portal sends ECP authn request and delegatable assertion to the IdP
4. IdP authenticates the portal via the delegatable assertion
5. IdP issues a delegated assertion within the ECP response to the portal
6. Portal sends the ECP response to the portlet
7. Portlet validates delegated assertion and returns the requested content back to the portal

Shibboleth Solution


IdP
Portal (WSC)
Portlet (WSP)
Delegatable Assertion from normal Shib authn request
Request for content
ECP Authn Request returned on HTTP Response
Attached Delegatable Assertion
ECP Authn Request with Delegatable Assertion
Verify Delegtable Assertion
ECP Authn Response with Delegated Assertion
ECP Authn Response with Delegated Assertion on HTTP Request
Returned Content on HTTP Response

Shibboleth Solution: Security

- IdP, Portal, and all Portlets must be SAML entities and registered in SAML metadata
- Issuing IdP added to delegatable assertion's audience list
  - prevents the assertion from being used with any other IdP
- Delegated assertion uses holder-of-key subject confirmation (instead of bearer)
  - ensures only entities with the private key can use the assertion
  - prevents assertion hijacking (unless the key is hijacked as well)
- Delegated assertion contains delegation restriction condition
  - prevents the assertion from working with SPs that do not support delegation (in theory at least)
- ECP Authn response may be encrypted so that the portal can not view information targeted for the portlet

Shibboleth Solution: IdP Setup

- Install N-Tier plugin in to IdP 2.1.3+
- Replace existing SAML2SSO profile with version that supports delegation and configure
- Add ECPSSO profile and configure
- Configuration Options:
  - SPs allowed to request delegatable assertion
  - Maximum delegation chain length
  - Lifetime of delegated assertion
  - SPs to which an assertion may be delegated

Shibboleth Solution: SP/WSP

- Install latest version of SP

Future Work Needed

- The current solution is use case specific - by design
  - Support for n-tier in all imaginable uses cases is hard
- A login handler that accepts, and validates, the user’s initial credentials
  - The current mechanism expects the whole flow to start with a browser interaction and thus it can use the existing login handlers
- A set of web service clients
  - The WSC is a Java library based on Apache HTTPClient
    - ❑ The WSC is not uPortal specific
  - But a good library (or two) for other common languages is needed

Resources

- Shib-uPortal Work Site:

  https://spaces.internet2.edu/display/ShibuPortal/Home

- uPortal WSC Code:

  https://www.ja-sig.org/svn/sandbox/ShibbolethuPortalIntegration

- IdP Plugin Code

  https://svn.middleware.georgetown.edu/shib-extension/java-idp-delegation