OpenId Connect Support in Shibboleth Identity Provider

David Langenberg
University of Chicago

Misagh Moayyed
Unicon, Inc

THE UNIVERSITY OF CHICAGO

Objective

- OpenId Connect support @ Shibboleth Identity Provider
- Use license/compatible open-source tools/ libraries
- Abide by the Identity Provider design guidelines
- Contribute back to the community/platform

Initial Scope

- Authorization code workflow
- OIDC RP administration within the IdP
- Resolve/Release claims via IdP's attribute resolution machinery
- Configuration of expiration/revocation policy around OIDC access/refresh tokens

Planned

- Implicit/Hybrid workflows
- Dynamic discovery
- Dynamic RP registration
- Logout
- UI enhancements

How

- MITREid Connect https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server

  - Spring/Maven environment, Apache v2 licensed

  - Based on Spring Security / Spring OAuth

Protocol Overview

- Endpoints:
  - `/idp/profile/oidc/authorize`
  - `/idp/profile/oidc/token`
  - `/idp/profile/oidc/userinfo`
  - `/idp/profile/oidc/jwk`

Configuration

- `conf/oidc-protocol.xml`
- `conf/relying-party.xml`
- `credentials/keystore.jwks`

Demo

Are we there yet?

- OIDC claims via IdP attribute encoding
- OIDC RP registration via IdP configuration

On Github

https://github.com/uchicago/shibboleth-oidc

** Modeled as a Maven overlay*

Q/A

David Langenberg
davel@uchicago.edu

Misagh Moayyed
mmoayyed@unicon.net

UNICON®

THE UNIVERSITY OF CHICAGO