

OIDC plugin for Shibboleth IdP Status Update 25/June/2019

Henri Mikkonen, Janne Lauros
CSC – IT Center for Science Ltd.



Sprint work items – Preparing version 1.1.0

- New features
 - OAuth2 introspection endpoint
 - <https://tools.ietf.org/html/rfc7662>
 - AppAuth – client SDK for native apps
 - PKCE extension for OAuth - <https://tools.ietf.org/html/rfc7636>
- Minor bug fixes
 - Client-side storage of user sessions failing
 - <https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues/24>

Sprint work items – Towards upstream integration (recap)

- Continued designing improvements for the trusted application metadata management for OIDC applications
 - Currently trust relationships are managed via JSON files
 - File format taken from the OIDC dynamic client registration spec
- Shibboleth IdP already supports SAML **and CAS** configuration via SAML metadata
 - This approach offers uniform configuration style for
 - basic information (unique id, endpoints)
 - trusted keys
 - attribute policies
 - ...

Sprint work items – OIDC XML metadata draft example

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Name="RP test">
  <md:EntityDescriptor entityID="mockClientId">
    <md:RoleDescriptor xmlns:oidcmd="urn:TODO:oidcmd"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="oidcmd:OAuthRPRoleDescriptorType"
        protocolSupportEnumeration="urn:TODO:oidc"
        oidcmd:TokenEndpointAuthMethod="client_secret_basic">
      <oidcmd:RedirectUri>https://example.org/cb</oidcmd:RedirectUri>
      <oidcmd:RedirectUri>https://example.org/cb2</oidcmd:RedirectUri>
      <oidcmd:GrantType>authorization_code</oidcmd:GrantType>
      <oidcmd:ResponseType>code</oidcmd:ResponseType>
      <oidcmd:ApplicationType>web</oidcmd:ApplicationType>
    </md:RoleDescriptor>
  </md:EntityDescriptor>
</md:EntitiesDescriptor>
```

Coming up next

- Summer break (whole July)
- Finish the OpenID Certification
- Patching as needed
- Continue collaboration with the Shibboleth team