OIDC plugin for Shibboleth IdP
Status Update 14/May/2019

Henri Mikkonen & Janne Lauros

CSC – IT Center for Science Ltd.

GÉANT
Networks · Services · People

Sprint work items – 2 patch releases

- Two patches after the first official release (1.0.0, 2nd April 2019)
  - 1.0.1:
    - Added missing key identifier for JWE header
      - https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues/16
  - 1.0.2:
    - Fixed claim parameter parsing error for request objects
      - https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues/21
    - Improved client logo handling for IdP UI (login page)
      - https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues/20
    - Improved configuration for discovery and keyset flows
      - https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues/18

Sprint work items – Towards upstream integration

- Started 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
    - …

Coming up next

- Patching as needed

- OAuth2 introspection endpoint

- Continue collaboration with the Shibboleth team

- Related work (not done in the incubator task, a plugin for this plugin):
  - https://github.com/CSCfi/shibboleth-idp-oauth2-deviceflow-extension