OpenID Connect for Swiss edu-ID

SWITCH

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

What is OpenID Connect?

- OAuth 2.0: authorisation protocol for applications
- Adds “simple identity layer” on top of OAuth 2.0
- Easy solution for delegating access to protected resources
- Reinvents the wheel with JSON (see JW*)
- OpenID Connect 1.0 finalised early 2014
- Popular with web and mobile developers

Meanwhile, in our community...

- Very few concrete use cases for OAuth or OIDC so far
- SAML isn't going away soon
- Bridging SWITCHaai and OIDC is technically possible, see our example mobile proxy (https://www.switch.ch/aai/support/tools/aai-for-apps/)

Operate SAML and OIDC together

- Ask each institution to operate an OIDC service?
  ⇒ rollout too slow
- One IdP with OIDC for the whole federation
  ⇒ the Swiss edu-ID IdP!

Pilot IdP with OpenID Connect

- Shibboleth IdPv3 addon (https://github.com/uchicago/shibboleth-oidc) developed by the University of Chicago and Unicon
- Successfully tested by another team @SWITCH
- Open for other testers
- Manual client registration
- Contact us if you want to try

Other interesting projects

- Mapping eduPerson attributes to OIDC claims
  REFEDS OIDCre WG
  (https://wiki.refeds.org/display/GROUPS/OIDCre)
- OpenID Connect Federation draft
  (https://github.com/rohe/pyoidc/blob/master/oidc_fed/oidcfed.txt)