

Re-booting OIDC Sweden

Martin Lindström – martin@idsec.se

Agenda

- Re-cap
- Introduction for new participants
- What has happened since last?
- Where should we publish our specifications?
- Things left to do
- What we shouldn't do
- CIBA – Include or not?
- Plans for Sweden Connect

What has happened since last?

- DIGG has announced that Sweden Connect should be extended to support OIDC
 - Should be built upon our work
 - “Aggressive” planning – November 2022
 - Martin will actually get paid to work with this ...
- CIBA has emerged
 - Pretty much 1-to-1 mapping of BankID’s and Freja’s API:s with polling

Where should we publish?

- www.oidc.se is not enough – We need to publish our specifications somewhere to get an independent organization behind our work.
- Kantara
 - Leif has initiated a dialogue
- OpenID Foundation (OIDF)
- IETF secdispatch - <https://datatracker.ietf.org/wg/secdispatch/about/>
- Create own association
- Last resort: Let DIGG host the specifications
 - Will not be independent

Things left to do ...

- Complete “The Swedish OpenID Connect Profile” (main spec)
 - Not far from finished. Need more work on metadata (discovery and registration) and also security requirements.
 - Define some new values for registration (e.g. type, contract) ...
- Complete “Attribute Specification for the Swedish OAuth2 and OpenID Connect Profiles”
 - Remove claims specific to Sweden Connect/eIDAS.
- Remove “Vector of Trust Registry”
 - Let it mature first. Could be introduced later.

Things left to do ... (cont.)

- Re-write “Signature Extension for OpenID Connect”
 - The federated signing model is too specific to be included in this spec (handle it in Sweden Connect-context)
- Optional. Complete a version of “Cookbook for using the Swedish OpenID Connect Profile”.
- CIBA - Client-Initiated Backchannel Authentication Flow
 - Something for us at this stage?
- Implementations and testing ...

What we shouldn't do

- Federation support
 - Should be done within Sweden Connect (and other federations)
- Define sector specific claims
- Vectors-of-trust
- Look to deep into eIDAS 2 (Wallet)

CIBA – Include or not?

- OpenID Connect Client-Initiated Backchannel Authentication Flow
 - https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html
- A perfect match for “direct” integration against BankID and Freja?
- Profile the specification and include it as an optional feature to the main profile?

Plans for Sweden Connect

- Profiles built upon our work
 - Sweden Connect also needs to revise the specs for signature services
- Profiles for OIDC federation (registration and discovery)
- Processes for joining the OIDC federation
- Metadata registry according to new specs
- Testing tools and other support
- A SAML to OIDC proxy?
- Documentation and education