OAuth 2.0 Token Exchange

An STS for the REST of Us

Brian Campbell et al.

IETF 96
Berlin
July 2016

Just One Example
(a quick illustration in the very unlikely event of some folks not having read the draft)
Current Status

- Draft -05 published July 8 (yes, the cut-off) with relatively minor changes
  - Added "cid" JWT claim that can express the client identifier of the client that requested the token.
  - Token introspection response parameter registration for "act" and "may_act"
  - refresh_token now OPTIONAL (was NOT RECOMMENDED)
  - Attempt to better clarify the distinction between JWT and access token URIs.
  - Remove some of the ‘Open Issues’
    - No short names
    - No supplementary info/claims
Moving Forward

- I believe it’s getting close…

Open Issues
- Facilitating proof-of-possession cases
  - In & out, token binding, use-case diversity

Other stuff
- ID Tokens
- URI
- Scope & “id_token” response parameter
- The title…