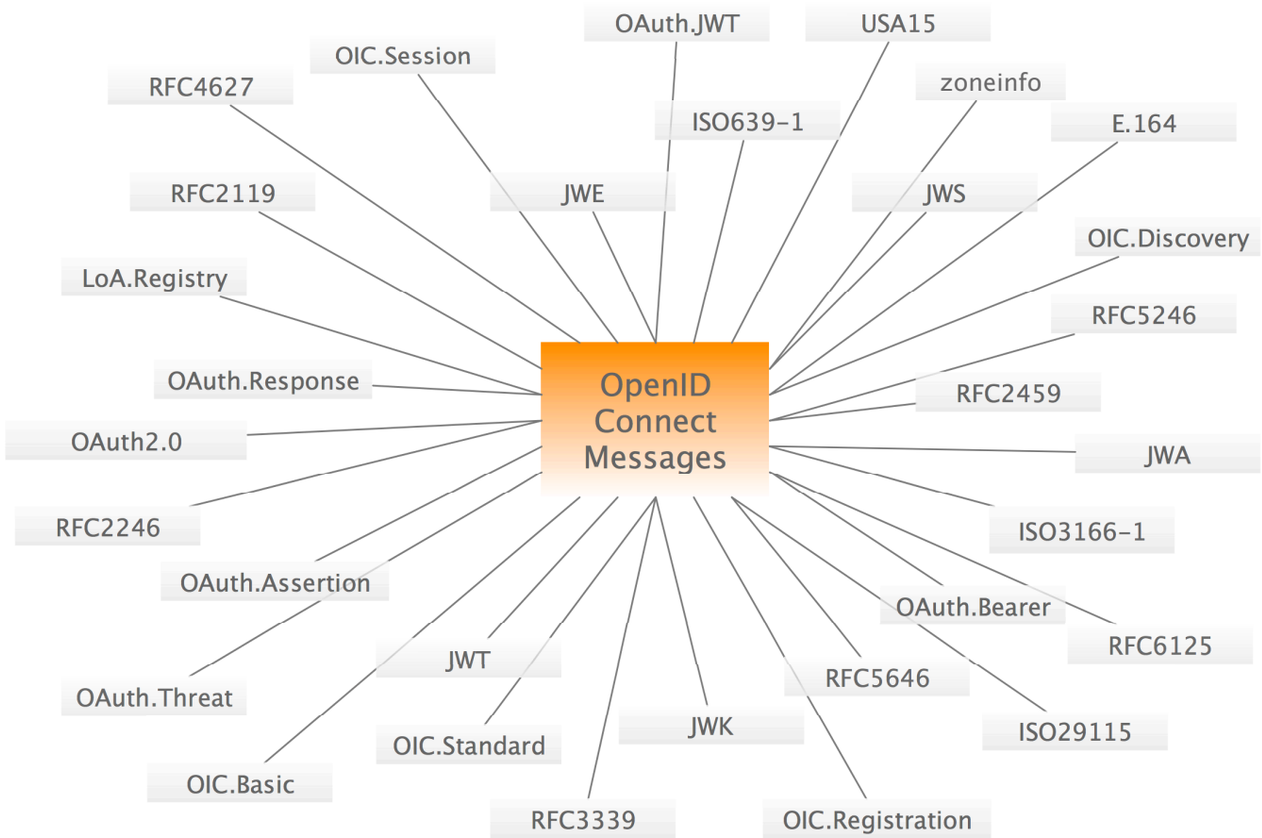
OpenID Connect Deployment Verification Tool

Roland Hedberg, ITS, Umeå University, Sweden
<roland.hedberg@adm.umu.se>

Implementing a standard

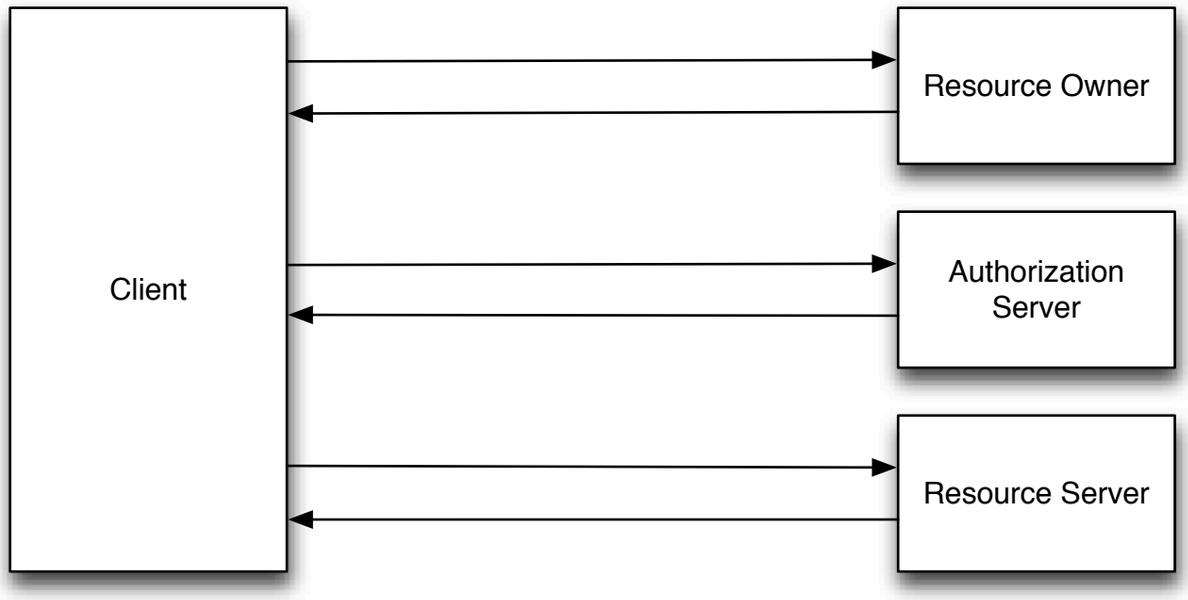
- Read and understand all relevant documentation
- The standard texts has to be cristal clear. There should be no room for ‘interpretations’
- Implementor ‘profiles’ appear



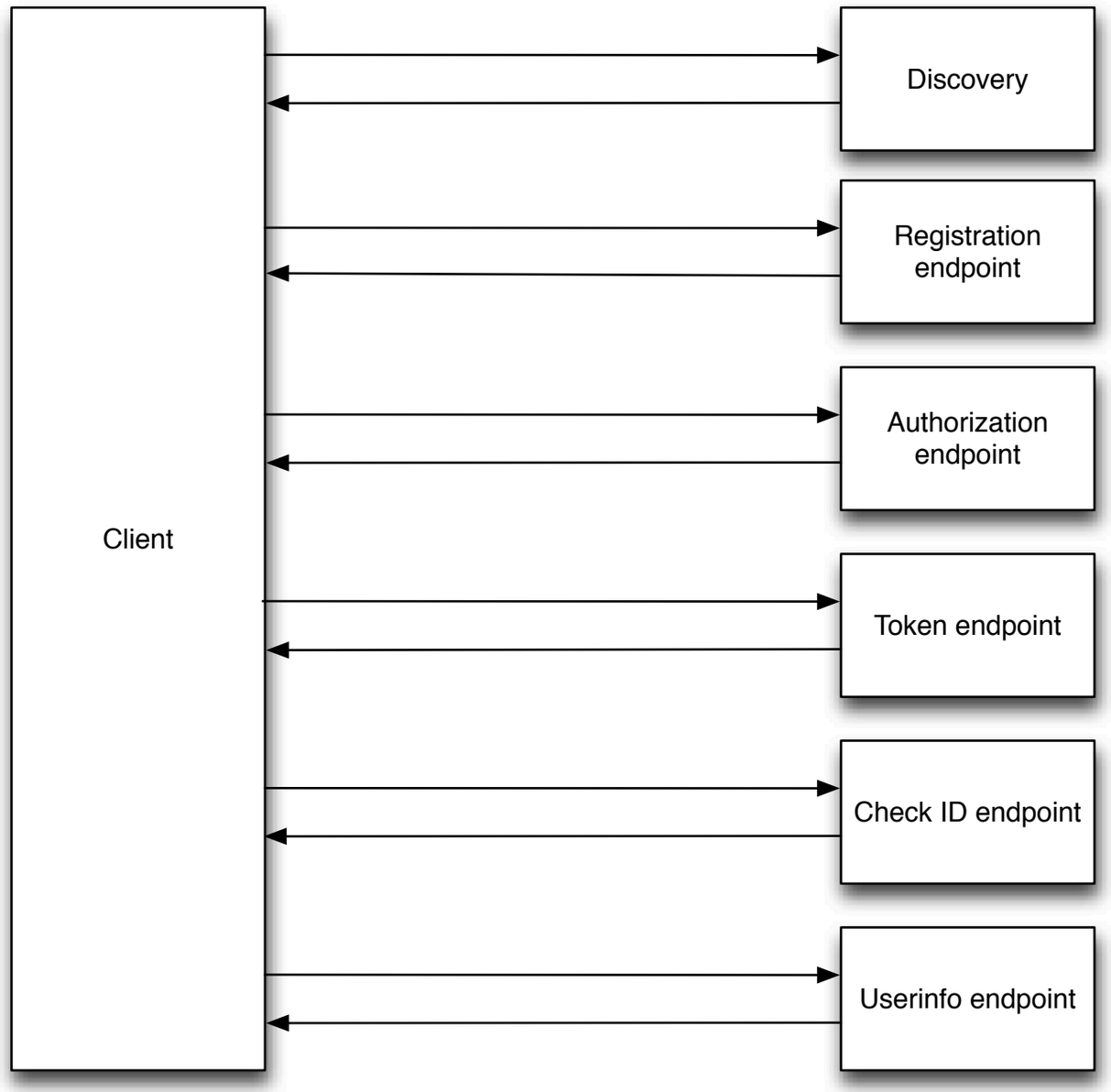
Promoting interoperability

- Verify that all the implementers has a common view of the standard
- How ?
    - Common forum
    - Interop meetings
    - Reference implementation

OAuth2 Abstract Protocol Flow

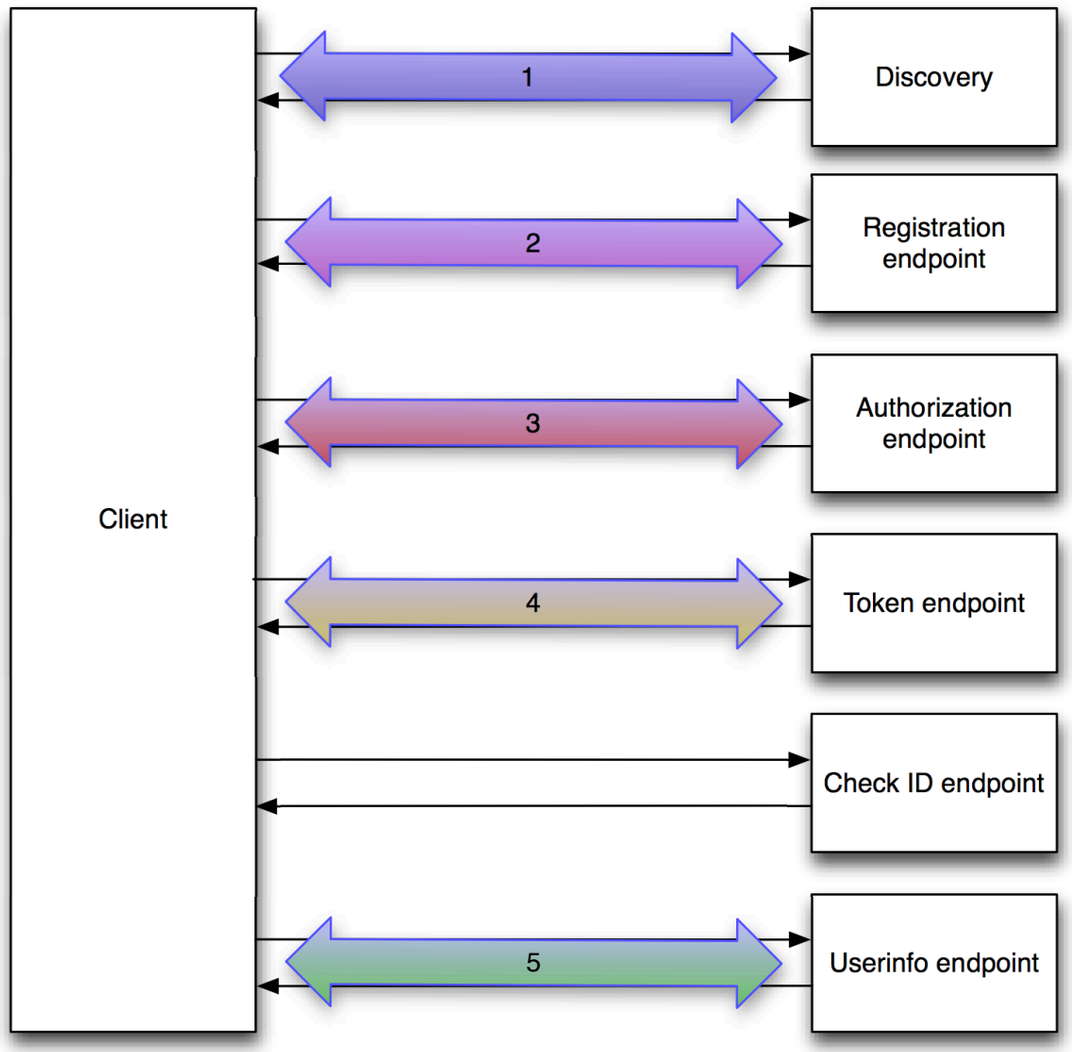


OpenID Connect endpoints



OpenID Connect flows

- Sequence of request - response pairs



Overall tool design

- Backend (me)
    - Does all the protocol handling
    - Maintains the flow definitions
    - Able to to some extent fake user interactions
    - Implemented as command line scripts
- Frontend (Andreas Åkre Solberg, UNINETT)
    - Implementation registration
    - Server configuration
    - Test result display
    - Implementor interactions

Testing a single flow
$ ./ebay.py | oicc.py -J - 'mj-01'

Discovery

- {"status": 0, "message": {"registration_endpoint": "https://openidconnect.ebay.com/oreo/register.jsp", "userinfo_endpoint": "https://openidconnect.ebay.com/oreo/openidconnect/get-user-info.jsp", "token_endpoint_auth_types_supported": ["client_secret_basic"], "scopes_supported": ["openid", "email", "location"], "refresh_session_endpoint": "https://openidconnect.ebay.com/oreo/openidconnect/refresh-session.jsp", "token_endpoint": "https://openidconnect.ebay.com/oreo/token.jsp", "version": "3.0", "response_types_supported": ["token", "code", "code id_token", "token id_token"], "end_session_endpoint": "https://openidconnect.ebay.com/oreo/openidconnect/end-session.jsp", "authorization_endpoint": "https://openidconnect.ebay.com/oreo/authorize.jsp", "check_id_endpoint": "https://openidconnect.ebay.com/oreo/openidconnect/check-session.jsp", "issuer": "https://openidconnect.ebay.com"}, "id": "check", "name": "Provider Configuration Response"},

Registration

- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/register.jsp", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"}
- {"status": 0, "message": "{\"client_id\":\"o1hqe2m52v6925vr68m8jffru6\",\"client_secret\":\"6FEDD5C0642932E7C6185306D5F2D25225EF19A1\",\"expires_at\":900}", "id": "check", "name": "Registration Response"},
- {"status": 1, "id": "check_content_type_header", "name": "Verify that the content-type header is what it should be."},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/register.jsp", "response_type": "RegistrationResponse", "id": "response-parse", "name": "Parsing the response"},
- {"status": 1, "id": "check-response-type", "name": "Checks that the asked for response type are among the supported"},

AuthorizationRequest

- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/authorize.jsp?nonce=VgGJC79pwuBP&state=STATE0&redirect_uri=https%3A%2F%2Fsmultron.catalogix.se%2Fauthz_cb&response_type=code&client_id=o1hqe2m52v6925vr68m8jffru6&scope=openid", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/primary-auth/dummy-signin.jsp?ru=https%3A%2F%2Fopenidconnect.ebay.com%2Foreo%2Fvalidate-auth.jsp&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=checkid_setup&openid.return_to=http%3A%2F%2Fhead2toes.org%2Fsandbox%2Fopenid%2Flightopenid-lightopenid%2Fexample.php%3Fproxy%3Dhttps%3A%2F%2Fopenidconnect.ebay.com%2Foreo%2Fvalidate-auth.jsp&openid.realm=http%3A%2F%2Fhead2toes.org%2Fsandbox%2Fopenid%2Flightopenid-lightopenid%2Fexample.php&openid.ns.sreg=http%3A%2F%2Fopenid.net%2Fextensions%2Fsreg%2F1.1&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/validate-auth.jsp?openid.identity=test&username=test&password=password&user_id=np01&confirmation=n%2Fa&confirmationExpiry=4049", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/consent/consent-default.jsp", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/consent/consent-plain.jsp", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/validate-consent.jsp?consent_user_response=pending&consent_confirmation_nonce=F3DB97731912AB2AAE93B050ED1D58490CAF397057149AC63473D5123F9120BE&consent_scope=ID", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/sts/token.jsp", "id": "check-http-response", "name": "Checks that the HTTP response status is within the 200 or 300 range"},
- {"status": 1, "url": "https://openidconnect.ebay.com/oreo/sts/token.jsp", "response_type": "AuthorizationResponse", "id": "response-parse", "name": "Parsing the response"},
- {"status": 1, "id": "check-authorization-response", "name": "Verifies an Authorization response. This is additional constrains besides what is optional or required."}

Doing a sequence of flows
$ oic_flow_tests.py kodtest

---

* (mj-00)Client registration Request - OK
* (mj-01)Request with response_type=code - OK
* (mj-02)Request with response_type=token - OK
* (mj-03)Request with response_type=id_token - OK
* (mj-04)Request with response_type=code token - OK
* (mj-05)Request with response_type=code id_token - OK
* (mj-06)Request with response_type=id_token token - OK
* (mj-07)Request with response_type=code id_token token - OK
* (mj-08)Check ID Endpoint Access with GET and bearer_header - OK
* (mj-09)Check ID Endpoint Access with POST and bearer_header - OK
* (mj-10)Check ID Endpoint Access with POST and bearer_body - OK
* (mj-11)UserInfo Endpoint Access with GET and bearer_header - OK
* (mj-12)UserInfo Endpoint Access with POST and bearer_header - OK
* (mj-13)UserInfo Endpoint Access with POST and bearer_body - OK
* (mj-14)Scope Requesting profile Claims - OK
* (mj-15)Scope Requesting email Claims - OK
* (mj-16)Scope Requesting address Claims - OK
* (mj-17)Scope Requesting phone Claims - OK
* (mj-18)Scope Requesting all Claims - OK
* (mj-19)OpenID Request Object with Required name Claim - OK
* (mj-20)OpenID Request Object with Optional email and picture Claim - OK
* (mj-21)OpenID Request Object with Required name and Optional email and picture Claim - OK
* (mj-22)Requesting ID Token with auth_time Claim - OK
* (mj-23)Requesting ID Token with Required acr Claim - OK
* (mj-24)Requesting ID Token with Optional acr Claim - OK
* (mj-25a)Requesting ID Token with max_age=1 seconds Restriction - OK
* (mj-25b)Requesting ID Token with max_age=10 seconds Restriction - OK
* (mj-26)Request with display=page - OK
* (mj-27)Request with display=popup - OK
* (mj-28)Request with prompt=none - OK
* (mj-29)Request with prompt=login - OK
* (mj-30)Access token request with client_secret_basic authentication - OK
* (mj-31)Request with response_type=code and extra query component - OK
* (mj-32)Request with redirect_uri with query component - OK
* (mj-33)Registration where a redirect_uri has a query component - OK
* (mj-34)Registration where a redirect_uri has a fragment - OK
* (mj-35)Authorization request missing the 'response_type' parameter - OK
* (mj-36)The sent redirect_uri does not match the registered - OK
* (mj-37)Access token request with client_secret_jwt authentication - OK
* (mj-38)Access token request with public_key_jwt authentication - OK
* (mj-39)Trying to use access code twice should result in an error - OK
* (mj-40)Trying to use access code twice should result in revoking previous issued tokens - OK

On error the script displays a trace log

```
12.668836 ============================================================
12.669350 --> URL: https://openidconnect.info/connect/token
12.669361 --> BODY:
code=cd1334144763.64309fce10e4a09e393d8534e6b669ba51&client_secret=c2b1d262a7b71388e1045d97ec60e5ae71e2103c&grant_t
ype=authorization_code&client_id=44d8e8ec438f5fbbcb3757c3b9badba57cfd33f6&redirect_uri=https%3A%2F
%2Fsmultron.catalogix.se%2Fauthz_cb
12.669373 --> HEADERS: {'content-type': 'application/x-www-form-urlencoded'}
14.014840 <-- RESPONSE: <Response [200]>
14.015405 <-- CONTENT: {"access_token":"at13341447658a6ea9b033aaaf2153a951c9a2a5b7e5","token_type":"Bearer","expires_in":
3599,"refresh_token":"rt1334144765b8f1de4220645b7cd9f7ef153529b22a","scope":"openid","id_token":"eyJ0eXAiOiJKV1QiLCJhbGciO
iJIUzI1NiJ9.eyJpc3MiOiJodHRwczovL29wZW5pZGNvbm5lY3QuaW5mby8iLCJ1c2VyX2lkIjoiMSIsImF1ZCI6IjQ0ZDhlOGVjNDM4ZjVmYm
JjYjM3NTdjM2I5YmFkYmE1N2NmZDMzZjYiLCJleHAiOjEzMzQxNDgzNjQsImFjciI6IjAiLCJub25jZSI6InVPY3BPM1NaWTJLMiJ9.doa_igT6
E9n_LwWYaki9bVHx4uKPvXo3JsvB-jw12z4"}
14.017345 [AccessTokenResponse]: {'access_token': u'at13341447658a6ea9b033aaaf2153a951c9a2a5b7e5', 'id_token':
u'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczovL29wZW5pZGNvbm5lY3QuaW5mby8iLCJ1c2VyX2lkIjoiMSIsImF1Z
CI6IjQ0ZDhlOGVjNDM4ZjVmYmJjYjM3NTdjM2I5YmFkYmE1N2NmZDMzZjYiLCJleHAiOjEzMzQxNDgzNjQsImFjciI6IjAiLCJub25jZSI6InVP
Y3BPM1NaWTJLMiJ9.doa_igT6E9n_LwWYaki9bVHx4uKPvXo3JsvB-jw12z4', 'expires_in': 3599, 'token_type': u'Bearer', 'scope':
u'openid', 'refresh_token': u'rt1334144765b8f1de4220645b7cd9f7ef153529b22a'}
14.017442 ============================================================
14.017924 --> URL: https://openidconnect.info/connect/token
14.017934 --> BODY:
code=cd1334144763.64309fce10e4a09e393d8534e6b669ba51&client_secret=c2b1d262a7b71388e1045d97ec60e5ae71e2103c&grant_t
ype=authorization_code&client_id=44d8e8ec438f5fbbcb3757c3b9badba57cfd33f6&redirect_uri=https%3A%2F
%2Fsmultron.catalogix.se%2Fauthz_cb
14.017946 --> HEADERS: {'content-type': 'application/x-www-form-urlencoded'}
15.317201 <-- RESPONSE: <Response [400]>
15.317728 <-- CONTENT: {"error":"invalid_grant"}
15.317840 ============================================================
15.318200 --> URL: https://openidconnect.info/connect/userinfo?
15.318210 --> BODY: None
15.318226 --> HEADERS: {'Authorization': u'Bearer at13341447658a6ea9b033aaaf2153a951c9a2a5b7e5'}
16.614897 <-- RESPONSE: <Response [200]>
16.615404 <-- CONTENT: {"user_id":"1"}
```

DEMO

http://openidtest.uninett.no/connect-provider

Q and A