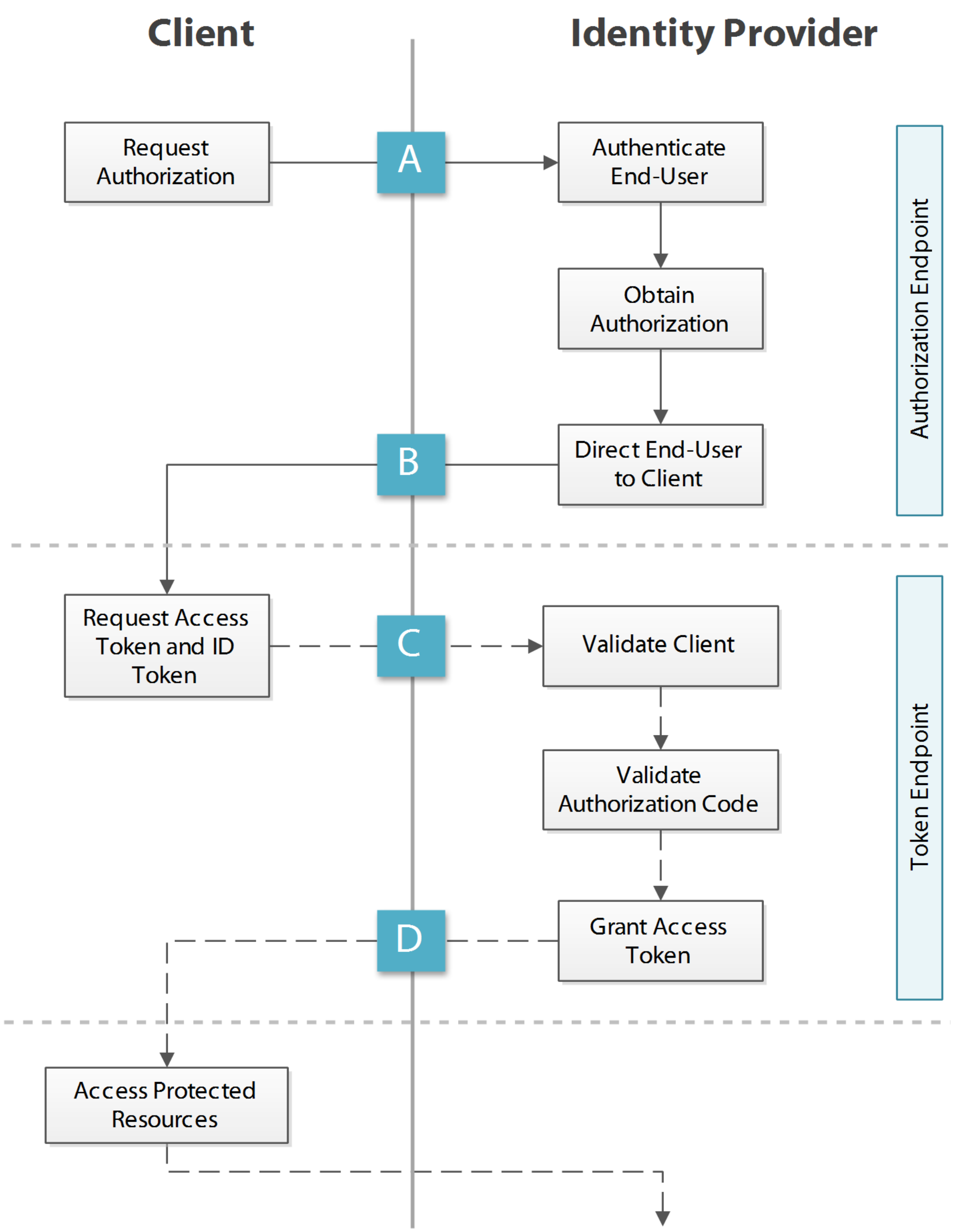
——→ Front Channel / Through User Agent

- - - → Back Channel / Direct Communication

OpenID Connect
Authorization Code Flow



A Client Requests Authorization

Request includes
response_type: `code`
scope: `openid` *(MAY include additional scopes)*
client_id
redirect_uri
state *(optional, recommended)*
nonce
display *(optional)*
prompt *(optional)*
request *(optional)*
request_uri *(optional)*

B Service Provider Grants Authorization

JSON response object (200 OK) includes
code
state *(required IFF state was sent in the request; must be equal to what was received)*

C Client Requests Access Token and ID Token

Request includes
grant_type: `authorization_code`
code
redirect_uri

If the client is confidential, it must authenticate with the Authorization Server in this request.

D Service Provider Grants Access Token and ID Token

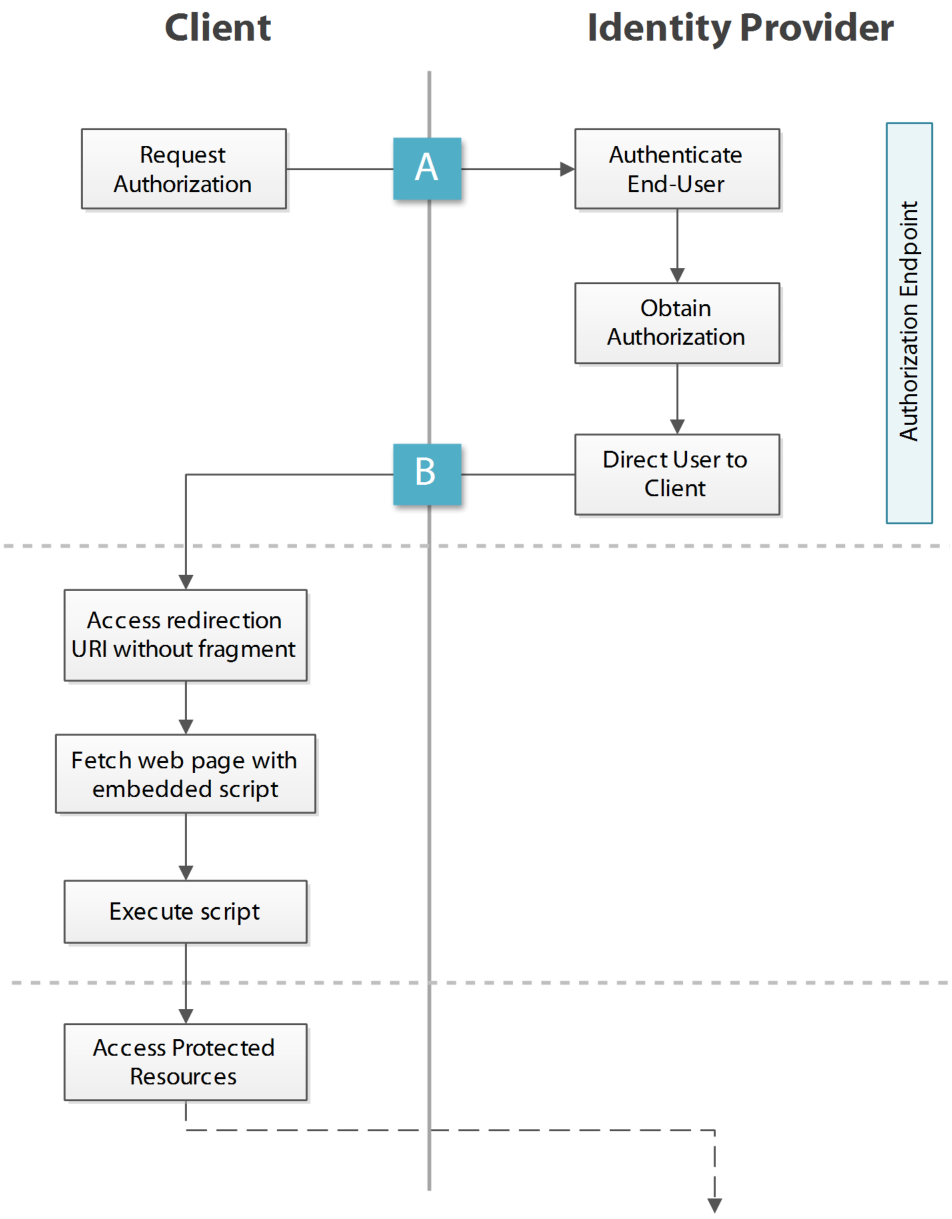
JSON response object (200 OK) includes
access_token
id_token
token_type: `Bearer`
expires_in *(optional)*
refresh_token *(optional)*
scope *(optional; SHOULD be included if the scope granted differs from the scope requested)*

——→ Front Channel / Through User Agent

– – – – – – → Back Channel / Direct Communication

OpenID Connect

Implicit Flow



A Client Requests Authorization

Request includes

response_type: `id_token token`
scope: `openid` *(MAY include additional scopes)*
client_id
redirect_uri *(required IFF the client has pre-configured more than one value with the service provider)*
state *(optional, recommended)*
nonce
display *(optional)*
prompt *(optional)*
request *(optional)*
request_uri *(optional)*

B Service Provider Grants Authorization

Redirection URI (302 Found) includes (url-encoded in fragment)

access_token
id_token
token_type: `Bearer`
expires_in *(optional)*
refresh_token *(optional)*
scope *(optional; SHOULD be included if the scope granted differs from the scope requested)*
state *(required IFF state was sent in the request; must be equal to what was received)*

→ Front Channel / Through User Agent

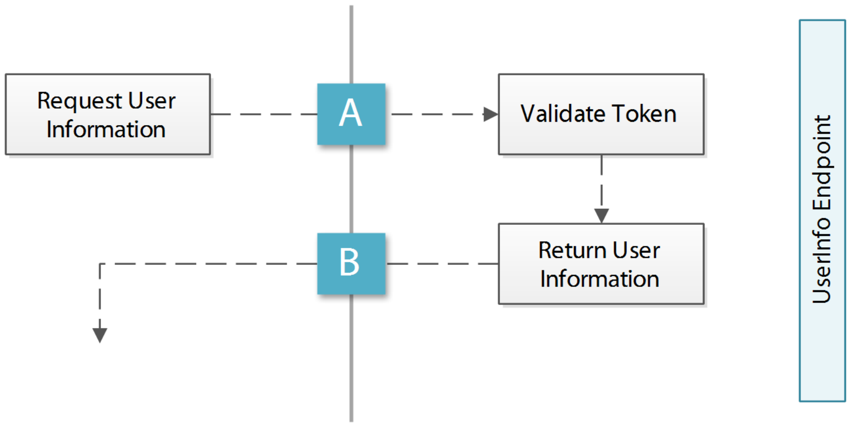
⇢ Back Channel / Direct Communication

OpenID Connect

Optional Steps

Client

Identity Provider



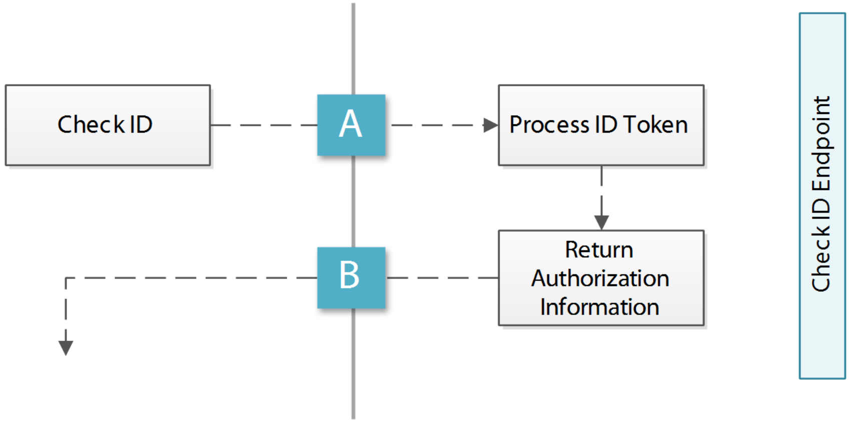
A **Client Sends**
UserInfo Request

Request includes
access_token
schema: `openid`

B **Service Provider Returns**
UserInfo Response

JSON response object (200 OK) includes
user_id

Optionally: name, given_name, family_name, middle_name, nickname, profile, picture, website, email, verified, gender, birthday, zoneinfo, locale, phone_number, address, updated_time



A **Client Sends**
Check ID Request

Request includes
id_token

B **Service Provider Returns**
Check ID Response

JSON response object (200 OK) includes
iss
user_id
aud
exp
iso29115 *(optional)*
nonce
auth_time *(optional)*

Created by: Amanda Anganes