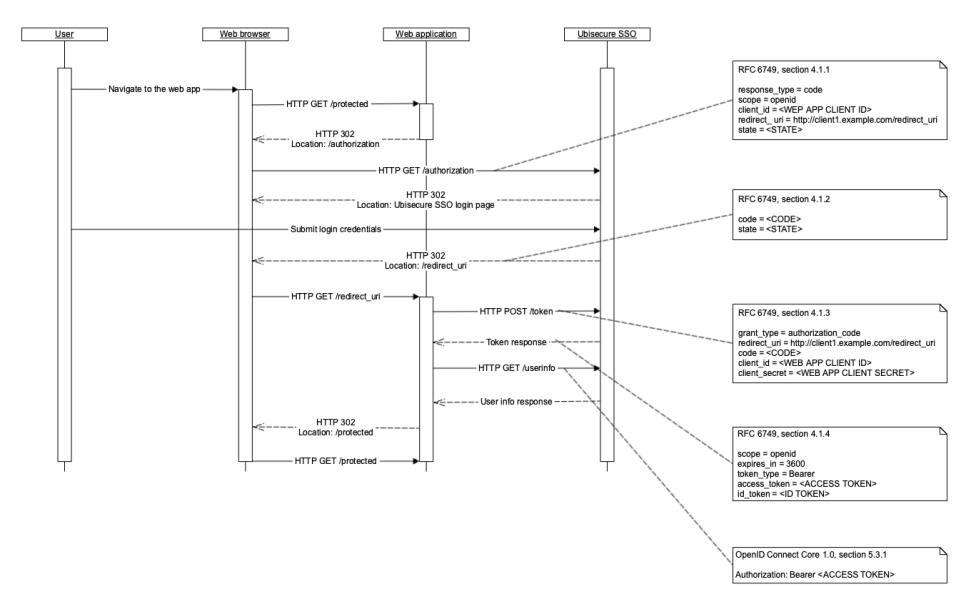
Authorization code grant and web single sign-on - SSO

In a web single sign-on use case a single OAuth Client is registered with SSO. This client is a web application running on a web server.

The client wants to get an access token for calling the userinfo service of SSO. The userinfo service returns claims and attributes describing the authenticated user.

Contents



Sequence diagram of authorization code grant

Authorization Request

https://tools.ietf.org/html/rfc6749#section-4.1.1
http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest

GET /uas/oauth2/authorization

Required Parameters

- response_type = code

  For authorization code grant the value must be set to "code"

- scope = openid

  For web single sign-on use case the value is set to "openid"

- client_id

  OAuth Client Identifier of the web application. This value is generated by SSO management when the OAuth Client is registered and activated. See Client registration and activation - SSO

- redirect_uri

  The redirect uri value must have been be registered with SSO management. The authorization server redirects the web browse to this address after authenticating the end-user. See Client registration and activation - SSO

Optional Parameters

- state

  An opaque value used by the client to maintain state between the request and callback

- nonce

  An opaque value used to associate a client session with an ID Token, and to mitigate replay attacks

- login_hint

  The value from login_hint is put into the username field on the login form

- acr_values

  Choose authentication methods that may satisfy the request.

- ui_locales

  Choose the locale used in the login form.

- max_age

  Specifies the allowable elapsed time in seconds since the last time the user was authenticated. If the elapsed time is greater than this value, the user is re-authenticated.

- prompt

  Possible values: *none, login, consent, select_acccount*. Value *none* means that the user is not shown a login page at all, which means that user won't be attempted to authenticate unless they already have an existing authentication. Values *login*, *consent* and *select_accou nt* all mean that user is always shown a login page, despite having an existing authentication or not.

- display

  Choose the UI template used in the login form. The template must contain the value of display parameter in the template setting *oidc. display*. For this setting, please refer to *Ubisecure SSO Login UI Customization*.

- code_challenge

  A challenge derived from the code verifier to be verified against when processing the subsequent token request. Required if a value is set for the key "code_challenge_method" in the Client Metadata. Otherwise optional.

  See RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients.

- code_challenge_method

  A method that was used to derive code challenge. Allowed values are "plain" and "S256". If not set, then the default value is the value of the key "code_challenge_method" in the Client Metadata if present, or "plain". Furthermore, if the value "S256" is set for "code_challenge_method" in the Client Metadata, the use of "plain" code_challenge_method in the authorization request is not allowed.

  See RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients.

Listing 1. Sample authorization request

```
GET
https://sso.example.com/uas/oauth2/authorization?
response_type=code&scope=openid&client_id=2001221477&redirect_uri=https://client.example.com
/response&state=40e1bfc0-4587-4859-be08-a58e3fffa37a&code_challenge=E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-
cM&code_challenge_method=S256
```

Authorization Response

https://tools.ietf.org/html/rfc6749#section-4.1.2
http://openid.net/specs/openid-connect-core-1_0.html#AuthResponse

Parameters

- code

  Authorization Code value generated by SSO

Optional Parameters

- state

  Value from authorization request

Listing 2. Sample authorization response

```
HTTP/1.1 302 Found
Location: https://client.example.com/response?state=40e1bfc0-4587-4859-be08-a58e3fffa37a&code=vn8DO49e%
2bZasXSaS7zTNlaiq5Zr9kNdgDbPubfaz7w%2bwgbxHXx8pmuL1F9gvX0id
```

Access Token Request

https://tools.ietf.org/html/rfc6749#section-4.1.3
http://openid.net/specs/openid-connect-core-1_0.html#TokenRequest

Replaying the same authorization code revokes the previously issued access token for the replayed authorization code.

POST /uas/oauth2/token

Required Parameters

- grant_type = authorization_code

  For token request with authorization code the value must be set to "authorization_code"

Allowed by Default.

- redirect_uri

  The value must be the same that was used for authorization request. See Authorization request.

- code

  Authorization Code value received in Authorization Response. See Authorization request.

- client_id & client_secret

  OAuth Client Identifier and Secret of the web application. See Client registration and activation - SSO

Optional Parameters

- code_verifier

  A cryptographically random string that is used to match the code_challenge sent in the authorization request to the token request.

  See RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients.

Listing 3. Sample token request

```
POST https://sso.example.com/uas/oauth2/token
Authorization: Basic MTc2MjQxNDM3NDoqKio=
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&redirect_uri=https://client.example.com
/response&code=QnKskjekHNhYlNKsD3pPKnJ4&code_verifier=dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk
```

Access Token Response

https://tools.ietf.org/html/rfc6749#section-4.1.4
https://tools.ietf.org/html/rfc6749#section-5.1
http://openid.net/specs/openid-connect-core-1_0.html#TokenResponse

Parameters

- scope = openid

  The requested scope value. See Authorization request.

- expires_in

  The lifetime in seconds of the access token

- token_type = Bearer
- access_token

  Access Token issued by the authorization server

Optional Parameters

- id_token

  If requested scope contains value "openid" then id_token is returned. However, id_token is not returned for refresh requests - i.e. when grant_type = refresh_token.

- refresh_token

  Refresh Token issued by the authorization server. The refresh token may be used in a refresh request to refresh the access token

  To see how the refresh token need to be set please refer to chapter OAuth 2.0 Client step 5 in Management UI Applications - SSO

Listing 4. Sample token response (JSON reformatted for readability)

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "scope": "openid",
    "expires_in": 3600,
    "token_type": "Bearer",
    "access_token": "DSJJU6QhquTUsznTDeDq0eVm",
    "id_token": "eyJhbGciOiJSUzI1NiJ9.eyJz…"
}
```

ID Token

http://openid.net/specs/openid-connect-core-1_0.html#CodeIDToken
http://openid.net/specs/openid-connect-core-1_0.html#IDToken

- sub

  Value that identifies the end-user

- iss

  Issuer of this response. Appears as "issuer" in authorization server metadata. See chapter Metadata Response in *OAuth 2.0 and OpenID Connect metadata - SSO*.

- aud

  OAuth Client Identifier of recipient

- exp

  Expiration timestamp

- iat

  Time at which this response was issued

- auth_time

  Time when end-user was authenticated

- amr

  Authentication methods reference, expressed as JSON array

- session_index

  SSO session index identifier

Optional Parameters

- acr

  Authentication context class reference. If context class is configured in SSO then value appears here

- nonce

  Value from authorization request. See Authorization request.

The ID Token may contain other name-value parameters (claims) as defined by SSO authorization policy.

UserInfo Request

http://openid.net/specs/openid-connect-core-1_0.html#UserInfoRequest

GET /uas/oauth2/userinfo

Required Parameters

- bearer authorization header Access Token value received in Access Token Response

Listing 5. Sample userinfo request

```
GET /uas/oauth2/userinfo HTTP/1.1
Host: sso.example.com
Authorization: Bearer DSJJU6QhquTUsznTDeDq0eVm
```

POST /uas/oauth2/userinfo

Required Parameters

- bearer authorization header Access Token value received in Access Token Response

Listing 5. Sample userinfo request

```
POST /uas/oauth2/userinfo HTTP/1.1
Host: sso.example.com
Authorization: Bearer DSJJU6QhquTUsznTDeDq0eVm
```

UserInfo Response

http://openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse
http://openid.net/specs/openid-connect-core-1_0.html#IDToken

Parameters

- sub

  Value that identifies the end-user

- iss

  Issuer of this response. Appears as "issuer" in authorization server metadata. See chapter Metadata Response in *OAuth 2.0 and OpenID Connect metadata - SSO*.

- aud

  OAuth Client Identifier of recipient

- exp

  Expiration timestamp

- iat

  Time at which this response was issued

- auth_time

  Time when end-user was authenticated

- amr

  Authentication methods reference, expressed as JSON array

- session_index

  SSO session index identifier

Optional Parameters

- acr

  Authentication context class reference. If context class is configured in SSO then value appears here

The userinfo response may contain other name-value parameters (claims) as defined by SSO authorization policy.

Listing 6. Example userinfo response (JSON reformatted for readability)

```
HTTP/1.1 200 OK
Content-Type: application/json
{
        "sub": "***",
        "iss": "https://sso.example.com/uas",
        "aud": "2001221477",
        "exp": 1429700671981,
        "iat": 1429697071971,
        "auth_time": 1429697071527,
        "amr": ["https://sso.example.com/uas/saml2/names/ac/password.1"],
        "session_index": "0a9b62ce8de4"
}
```