

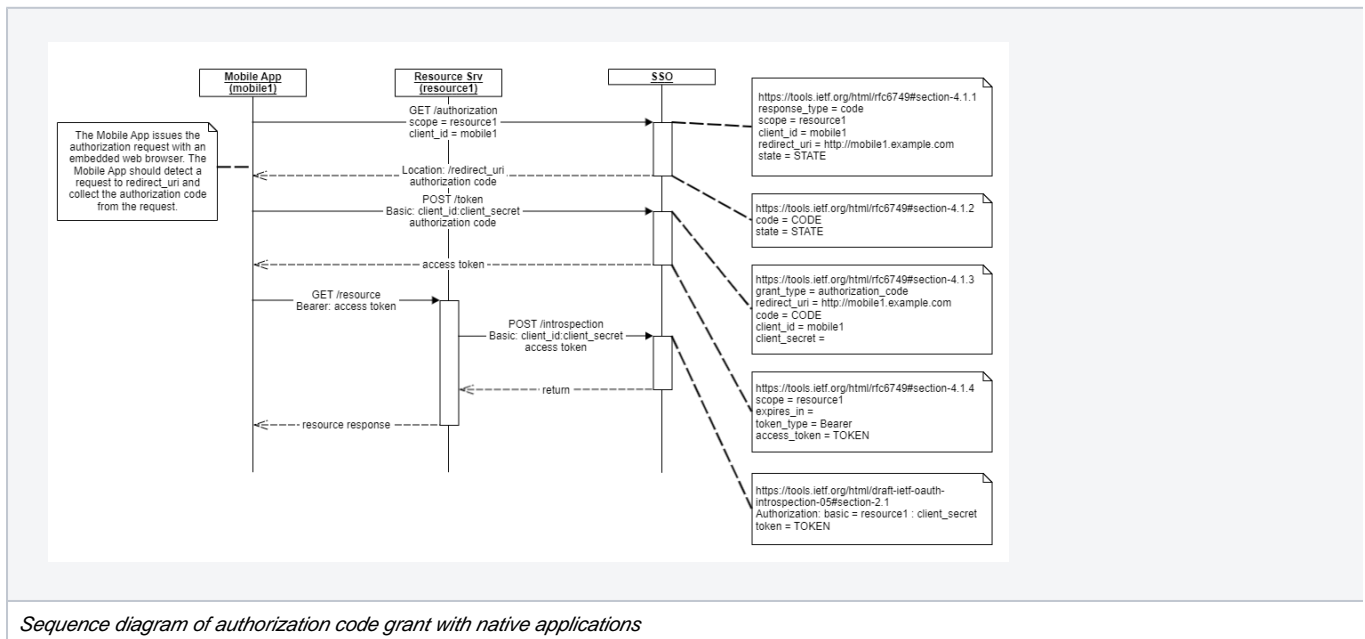
Authorization code grant and native applications - SSO

In a native application use case two OAuth clients are registered with SSO. The first client is the "native application" presenting user interfaces to the end-user. The second client is usually a web service or resource server providing API services to the native application.

The native application wants to get an access token for calling the resource server API services. The resource server validates the access token it receives by calling the introspection service. The introspection service returns claims and attributes describing the authenticated user.

Contents

- [Authorization Response](#)
- [Access Token Request](#)
- [Access Token Response](#)
- [Resource Server Request](#)
- [Token Introspection Request](#)
 - [POST /uas/oauth2/introspection](#)
- [Token Introspection Response](#)



Authorization Request

Instructions on page [Authorization code grant and web single sign-on](#)

Authorization Response

Instructions on page [Authorization code grant and web single sign-on](#)

Access Token Request

Instructions on page [Authorization code grant and web single sign-on](#)

Access Token Response

Instructions on page [Authorization code grant and web single sign-on](#)

Resource Server Request

<https://tools.ietf.org/html/rfc6750#section-2>

Required parameters

- access token Bearer authorization http header The application may alternatively choose to send the access token in a form or query parameter

Sample Resource server request

```
GET https://resource.example.com/api/method Authorization: Bearer DSJJU6QhquTUsznTDeDq0eVm
```

Token Introspection Request

<https://tools.ietf.org/html/rfc7662#section-2.1>

POST /uas/oauth2/introspection

Required parameters

- token
Access/Refresh Token value received by the resource server
- client_id & client_secret
OAuth Client Identifier and Secret of the resource server

Sample introspection request

```
POST https://sso.example.com/uas/oauth2/introspectionAuthorization: Basic MTc2MjJQxNDM3NDogKio=Content-Type: application/x-www-form-urlencoded token=DSJJU6QhquTUsznTDeDq0eVm
```

Token Introspection Response

<https://tools.ietf.org/html/rfc7662#section-2.2>

Parameters

- active
The value "true" if access token was valid
- aud
OAuth Client Identifier of the response recipient
- scope
Scope of the provided token. Subset of the scopes in the `scope` parameter given in the token request the token was generated for.
- client_id
OAuth Client Identifier of the client issuing the authorization request
- token_type
Type of the token submitted – `access_token` or `refresh_token`

In addition to the attributes listed above, the Introspection Response contains the same claims and attributes as the [UserInfo Response](#).

Sample introspection response

```
HTTP/1.1 200 OKContent-Type: application/json
\{"sub":"****","iss":"https://sso.example.com/uas","aud":"1762414374","exp":1429700671981,"iat":1429697071971,"auth_time":1429697071527,"amr":\["https://sso.example.com/uas/saml2/names/ac/password.1"\], "active":true,"scope":"openid 1762414374","client_id":"347937059","session_index":"0a9b62ce8de4","token_type":"access_token"\}
```