Authorization Code Grant

User

Click on a link

Website

Connect to
API Service

Facebook, Google,
Or your API

API Service

Authorization
Server

Authorization code request

?**response_type**=code&**state**={CSRF}&...

GET /authorize
  ?response_type=code   // Required. Must be "code"
  &state=hv8hf0h2i7d   // Recommended
  &redirect_uri= {Redirect uri}   // Optional
  &scope={Scopes}   // Optional
  &client_id={Client Id}   // Required

User

Click on a link →

Website

Connect to API Service

Facebook, Google, Your API

API Service

Authorization Server

Authorization code request

?**response_type**=code&**scope**={Scopes}&**state**={CSRF}
&redirect_uri=...

redirect_uri?**code={4hf7sn}**&**state**={CSRF}

```
POST https://{authorization-server-utl}/token
  ?grant_type=authorization_code
  &code={code}
  &redirect_uri={redirect-uri}
  &client_id={client_id}
  &client_secret={client_secret}
```

Response:
{
 "**access_token**" : "2YotnFZFEjr1zCsicMWpAA",
 "**expires_in**" : 3600
}

Authorization page

- Read photos
- Read videos

Username

Password

Allow

User | Website | Auth Server | Resource Server

1. Click the Login link

2. A request for authorization code.

/auth?client_id=photo-app-code-flow-client&response_type=code&scope=openid profile&redirect_uri=http://localhost:8083/callback&state=bG3Y7dl9Y6gD6

3. Present user with a Login page

4. User logs in

5. Present Consent Page

6. User authorizes website to access the requested information.

7. Authorization code

Redirect to http://localhost:8083/callback?code=99feb5f9-4707...

8. Exchange Authorization Code for an Access Token

HTTP Post /token + Code + Client ID + Client Secret

9. Response with an Access Token + Refresh Token

10. Request user data with an Access Token.

11. Validate token

12. Valid

13. Respond with a result