

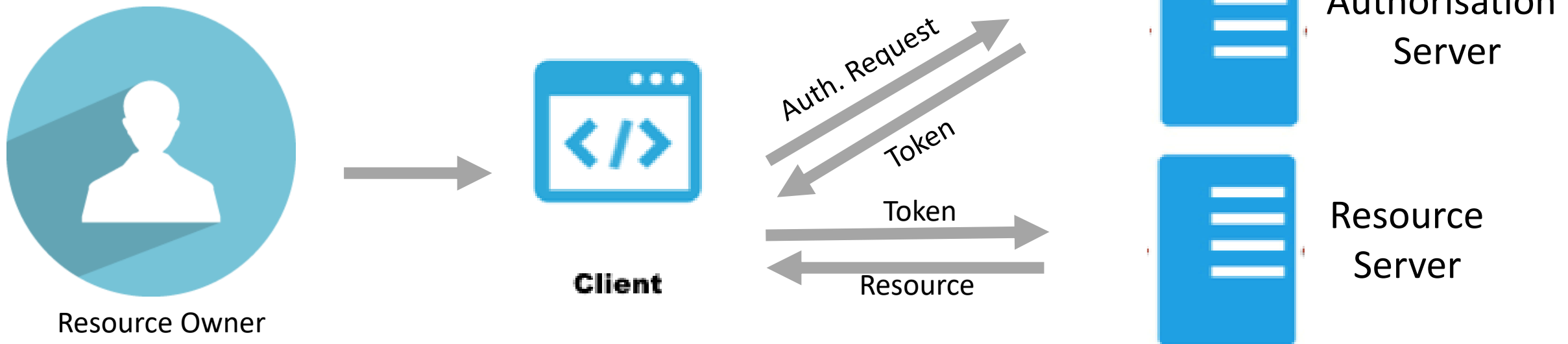
# OAuth 2 Introduction

---

- Roles
- Grant Types
- Flows
- Demo

# OAuth Roles

- **Resource Owner** ( User )
- **Client** ( Application that wants to access user account )
- **Resource Server** ( API ) Hosts User Accounts
- **Authorization Server** ( API ) Verifies the Identity

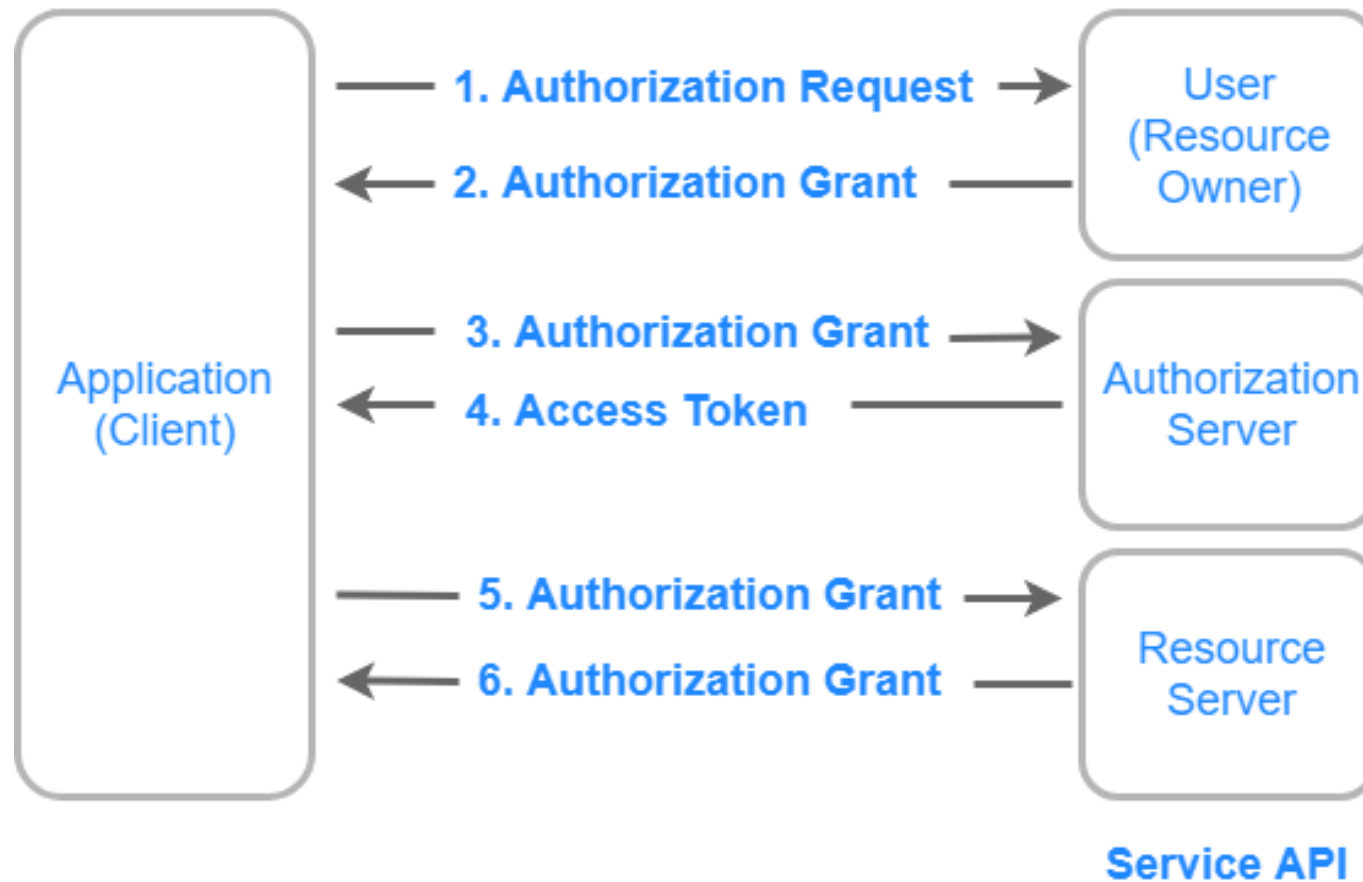


# Authorization Grant

- **1. Authorization Code:** used with server-side Applications
- **2. Implicit:** used with Mobile Apps or Web Applications (applications that run on the user's device)
- **3. Resource Owner Password Credentials:** used with trusted Applications, such as those owned by the service itself
- **4. Client Credentials:** used with Applications API access, example use case, changing application settings (authorization based on with client\_id, client\_secret)
- **5. Refresh token grant:** used to obtain an access token with a refresh token

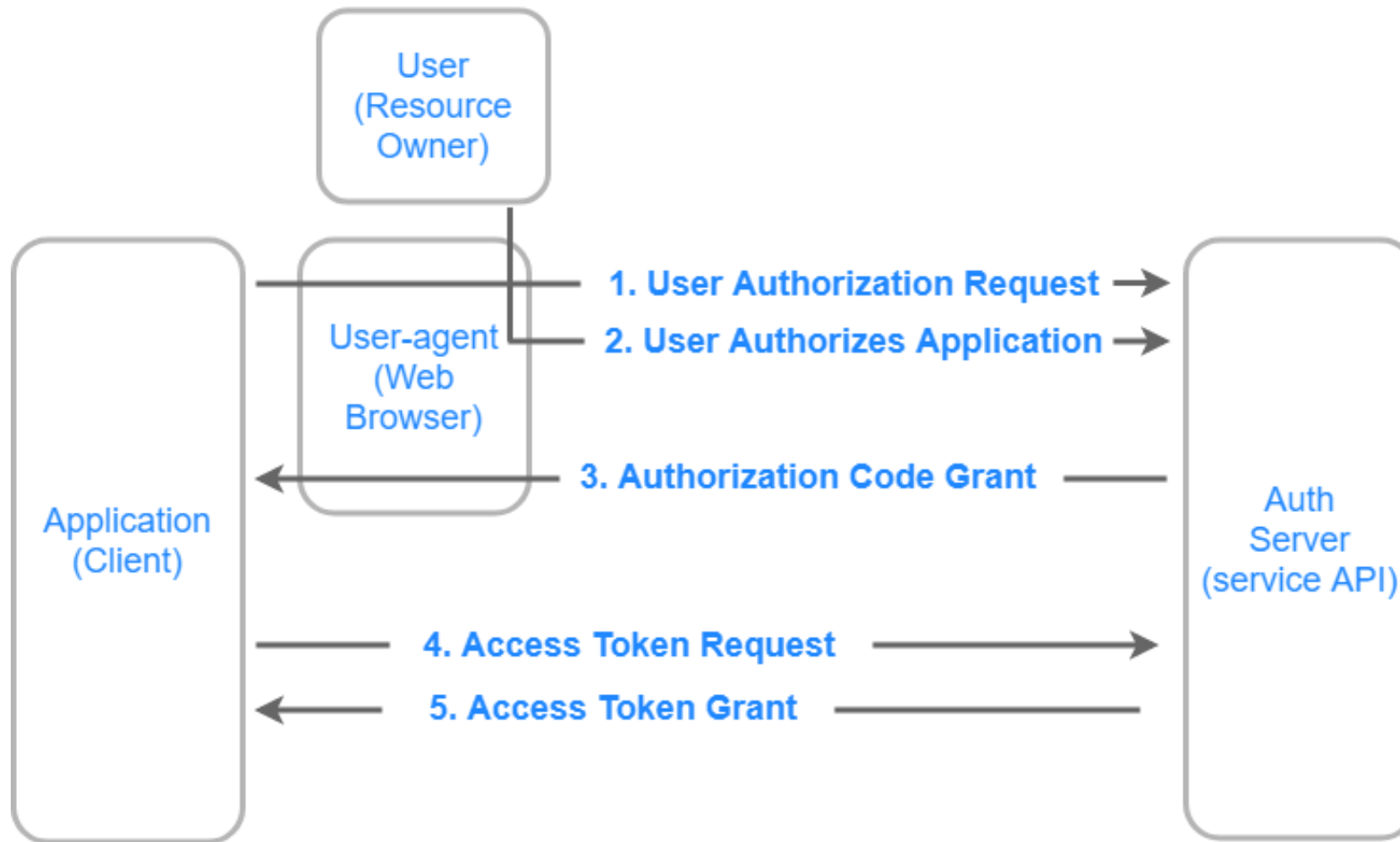
# General Overview

## Abstract Protocol Flow



# 1. Authorisation Code Grant Type

## Authorization Code Flow



# 1. Authorisation Code Grant Type

- 1. Application requests AUTHORISATION\_CODE

`https://cloud.digitalocean.com/v1/oauth/authorize?response_type=code&client_id=CLIENT_ID&redirect_uri=CALLBACK_URL&scope=read`

- 2. User authorizes
- 3. Application receives AUTHORISATION\_CODE

`https://dropletbook.com/callback?code=AUTHORIZATION_CODE`

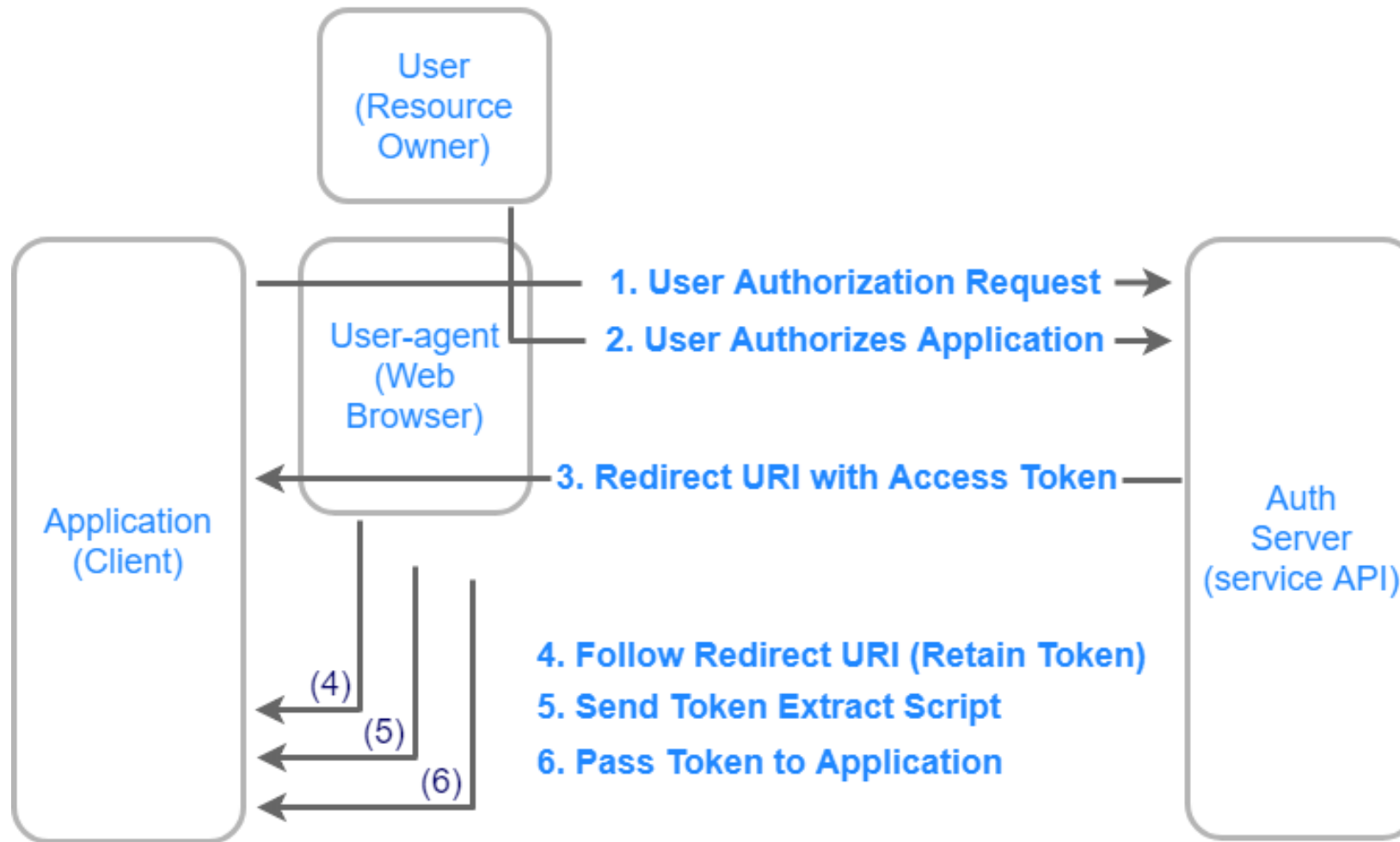
- 4. Application requests ACCESS\_TOKEN

`https://cloud.digitalocean.com/v1/oauth/token?client_id=CLIENT_ID&client_secret=CLIENT_SECRET&grant_type=authorization_code&code=AUTHORIZATION_CODE&redirect_uri=CALLBACK_URL`

- 5. Application receives ACCESS\_TOKEN

## 2. Implicit Grant Type

### Implicit Flow



## 2. Implicit Grant Type

### 1. Application requests authorisation

[https://cloud.digitalocean.com/v1/oauth/authorize?response\\_type=token&client\\_id=CLIENT\\_ID&redirect\\_uri=CALLBACK\\_URL&scope=read](https://cloud.digitalocean.com/v1/oauth/authorize?response_type=token&client_id=CLIENT_ID&redirect_uri=CALLBACK_URL&scope=read)

### 2. User Authorizes Application

- **Step 3: User-agent Receives Access Token with Redirect URI**

[https://dropletbook.com/callback#token=ACCESS\\_TOKEN](https://dropletbook.com/callback#token=ACCESS_TOKEN)

- **Step 4: User-agent Follows the Redirect URI**
- **Step 5: Application Sends Access Token Extraction Script**
- **Step 6: Access Token Passed to Application**



### 3. Grant Type: Resource Owner Password Credentials

#### 1. Requesting a Token Based on User Credentials

`https://oauth.example.com/token?grant_type=password&username=USERNAME  
&password=PASSWORD&client_id=CLIENT_ID`

## 4. Grant Type: Client Credentials

### 1. Requesting Token Based on Application Credentials

`https://oauth.example.com/token?grant_type=client_credentials&client_id=CLIENT_ID&client_secret=CLIENT_SECRET`

## 5. Grant Type: Refresh Token

### 1. Requesting Token Based on a Refresh Token

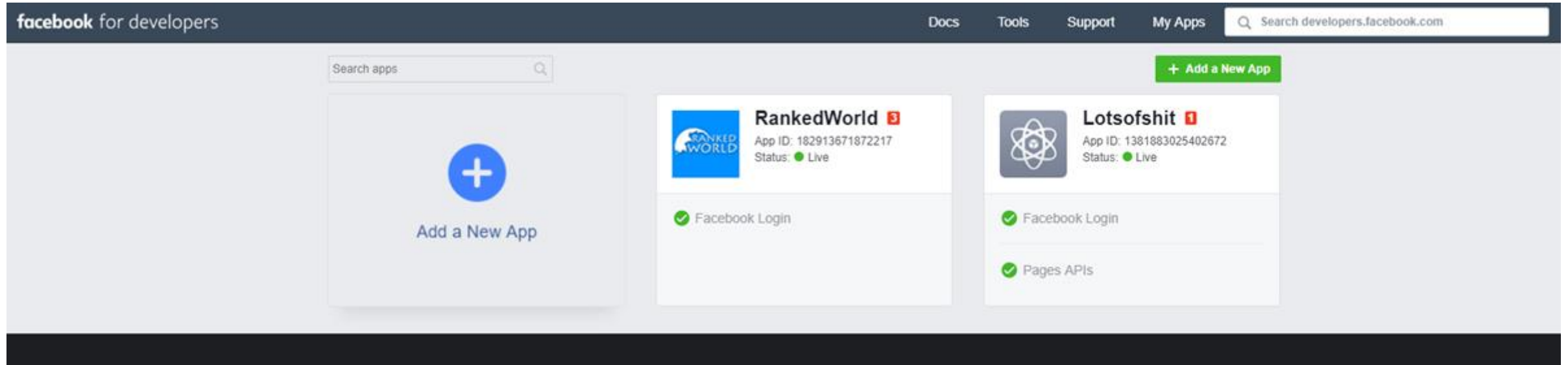
[https://cloud.digitalocean.com/v1/oauth/token?grant\\_type=refresh\\_token&client\\_id=CLIENT\\_ID&client\\_secret=CLIENT\\_SECRET&refresh\\_token=REFRESH\\_TOKEN](https://cloud.digitalocean.com/v1/oauth/token?grant_type=refresh_token&client_id=CLIENT_ID&client_secret=CLIENT_SECRET&refresh_token=REFRESH_TOKEN)

# facebook APP Configuration

---

1. Facebook APP Creation
2. Set Redirect URL
3. Facebook APP Configuration

# 1. Facebook APP Creation



## 2. Check Basic Information

**facebook** for developers

DocsToolsSupportMy Apps

Search developers.facebook.com

RankedWorld

APP ID: 182913671872217

ON

Status: Live

View Analytics

Dashboard

Settings

Basic

Advanced

Roles

Alerts 3

App Review

PRODUCTS +

Facebook Login

App Center

Activity Log

Editing Display Name is disabled because your App Center submission is pending review. To make changes, you can [review your submission here](#).

App ID

182913671872217

App Secret

.....

Show

Display Name

RankedWorld

Namespace

App Domains

rankedworld.net

Contact Email

support@rankedworld.net

Privacy Policy URL

http://rankedworld.net/privacy.php

Terms of Service URL

http://rankedworld.net/tou.php

App Icon (1024 x 1024)

1024 x 1024

Category

Entertainment

Find out more information about app categories here

Business Use

This app uses Facebook tools or data to

Support my own business

Provide services to other businesses

# 3. Facebook APP Configuration

facebook for developers

Docs

Tools

Support

My Apps

Search developers.facebook.com

RankedWorld

APP ID: 182913671872217

ON

Status: Live

View Analytics

Dashboard

Settings

Roles

Alerts 3

App Review

PRODUCTS +

Facebook Login

Settings

Quickstart

App Center

Activity Log



To improve security, please turn on **Enforce HTTPS**. [Learn More](#)

## Client OAuth Settings

Yes

Client OAuth Login

Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [?]

Yes

Web OAuth Login

Enables web-based Client OAuth Login. [?]

No

Enforce HTTPS

Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]

No

Force Web OAuth Reauthentication

When on, prompts people to enter their Facebook password in order to log in on the web. [?]

No

Embedded Browser OAuth Login

Enable webview Redirect URIs for Client OAuth Login. [?]

Yes

Use Strict Mode for Redirect URIs

Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

## Valid OAuth Redirect URIs

<https://aademo.tk/> <http://aademo.tk/> <http://www.aademo.tk/> [http://www.aademo.tk/logged\\_in.html](http://www.aademo.tk/logged_in.html)

No

Login from Devices

Enables the OAuth client login flow for devices like a smart TV [?]

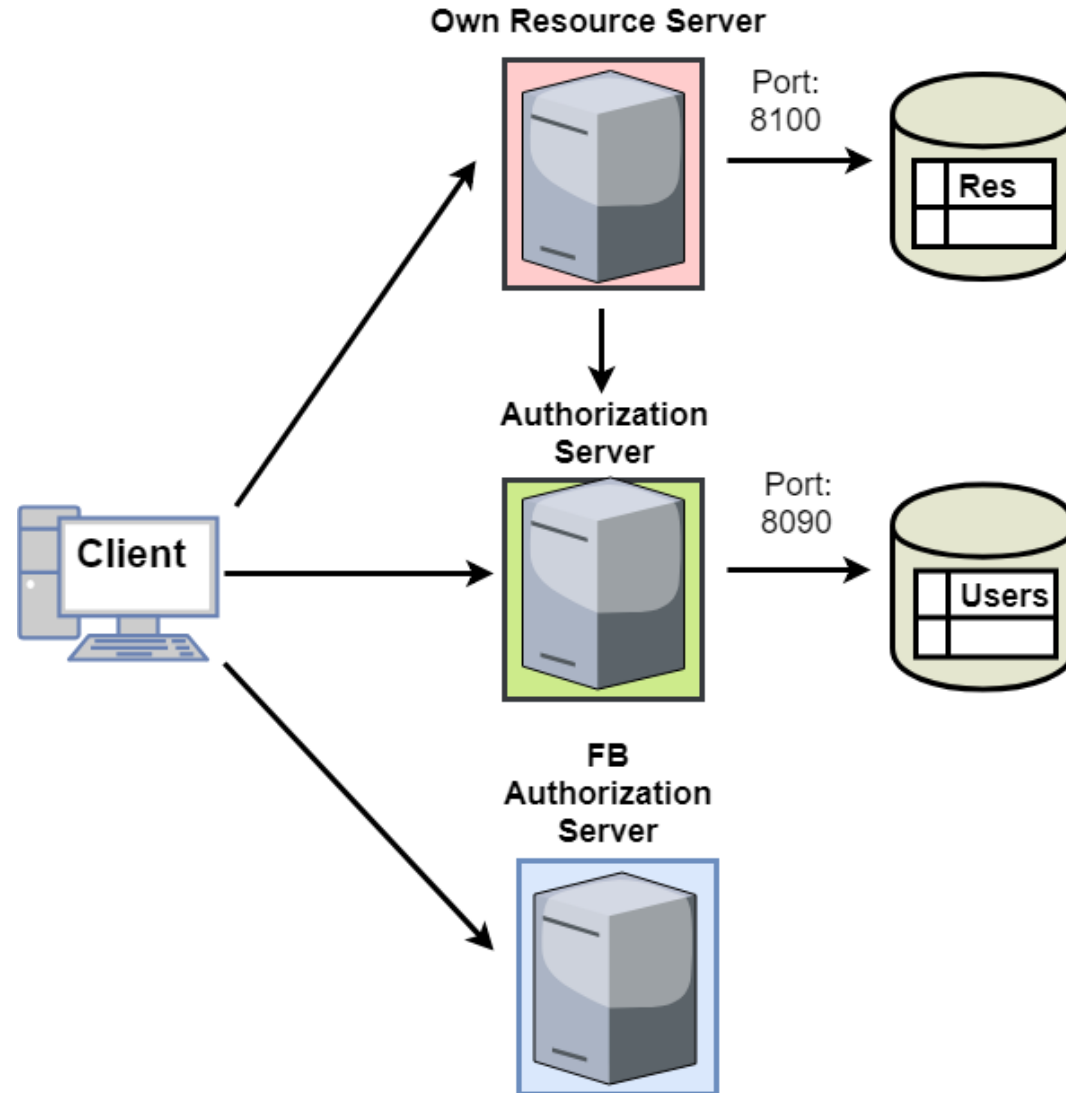
# OAuth MicroService Architecture Integration

---

1. General Overview
2. Implicit Flow
3. Authorization Code Flow

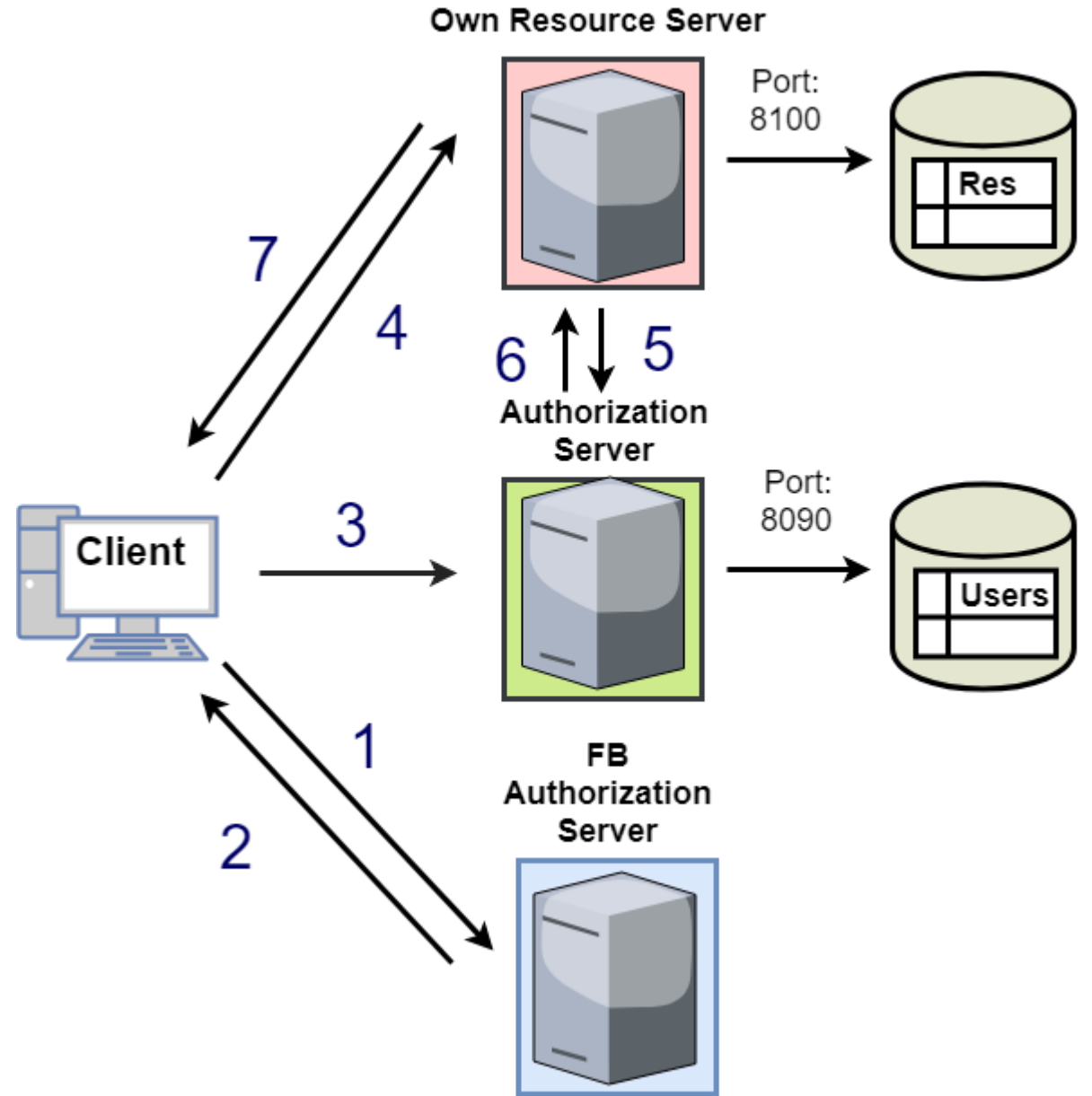


# 1. General Overview



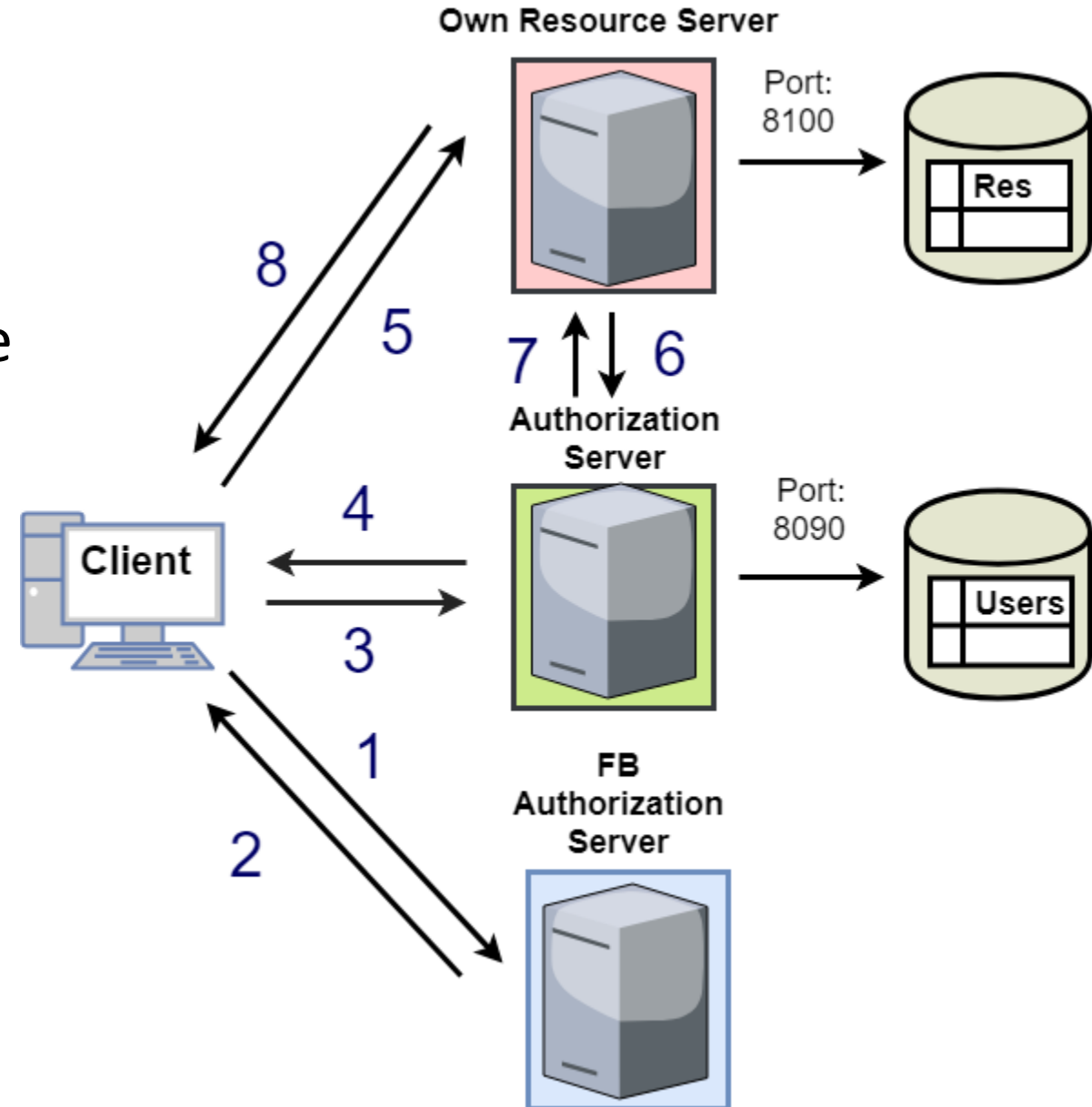
## 2. Implicit Flow

1. Access Token Request
2. User Receives Access Token
3. Client Registers User
4. Client Requests Resource
5. Resource Server Checks Token
6. Authorization Server Responds
7. User Receives Resource



### 3. Authorization Code Flow

1. Authorization Code Request
2. User Receives Authorization Code
3. Client Sends Auth Code  
(in the Background Code -> Token)
4. Client Receives App Token
5. Client Requests Resource
6. Resource Server Checks Token
7. Authorization Server Responds
8. User Receives Resource



# Auth Code – Access Token Exchange

- Request Authorization Code
- var `facebookAuthEndpoint` = "https://www.facebook.com/v2.10/dialog/oauth"  
+  
" ? response\_type= `code` " +  
"& client\_id= `182913671872217` " +  
"& redirect\_uri= `http://www.aademo.tk/logged_in.html`" +  
+ "& scope= `public_profile user_friends`";
- Request Access Token
- var `userEndpoint` = "https://graph.facebook.com/v2.10/oauth/access\_token?" +  
"client\_id=`182913671872217`&" +  
"redirect\_uri=`http://www.aademo.tk/logged_in.html`&" +  
"client\_secret=`b6b84d379d3d5006ecaf0eb2dd6f0cac`&" +  
"code=" + `code`;

# Demo

<http://www.aademo.tk>

# Thank You!

- Resources used:

- <https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2>
- <https://dzone.com/articles/oauth2-implicit-grant-flow-example-using-facebook>
- [https://developers.facebook.com/docs/php/howto/example\\_retrieve\\_user\\_profile](https://developers.facebook.com/docs/php/howto/example_retrieve_user_profile)
- <https://developers.facebook.com/docs/facebook-login/access-tokens>
- <https://developers.facebook.com/docs/facebook-login/manually-build-a-login-flow>

- Resources Created

- [https://github.com/kkocs/OAuth2\\_Demo](https://github.com/kkocs/OAuth2_Demo)