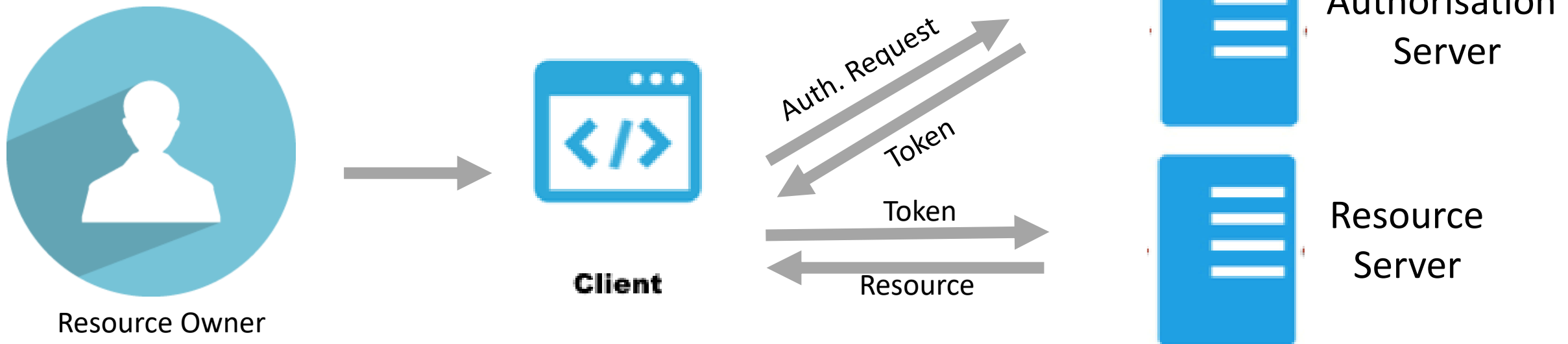


OUATH 2 Introduction

- 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

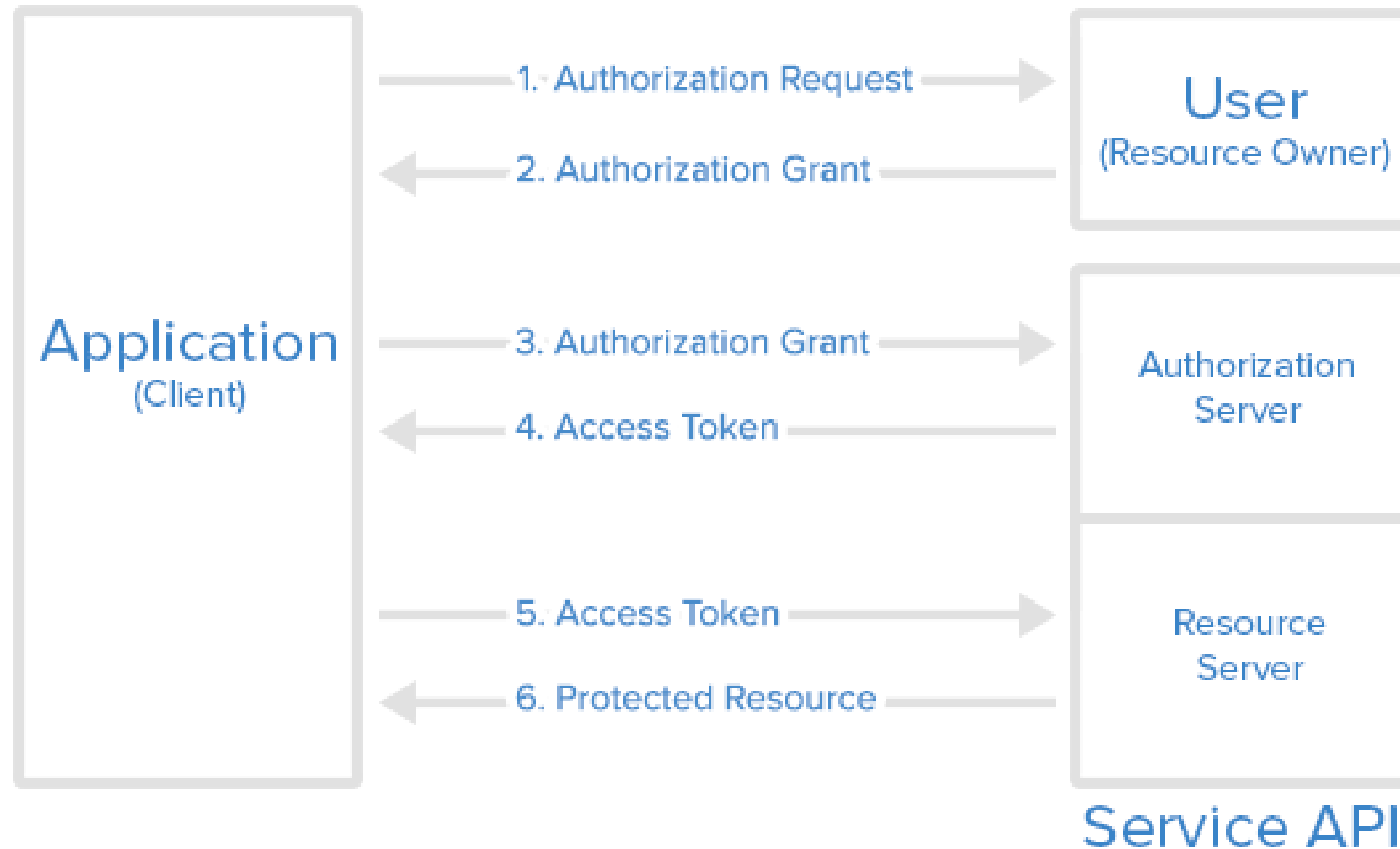


Authorization Grant

- **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

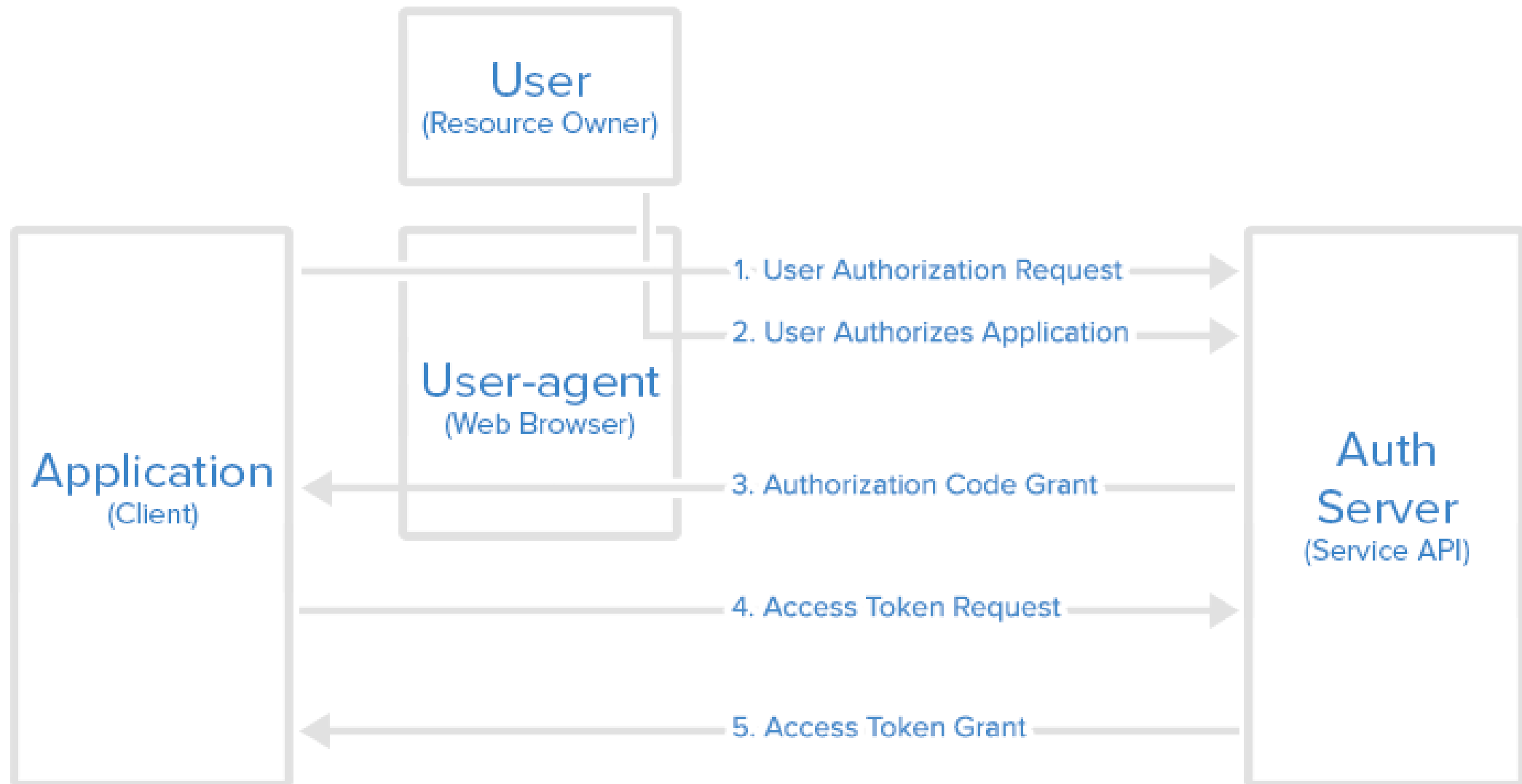
General Overview

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

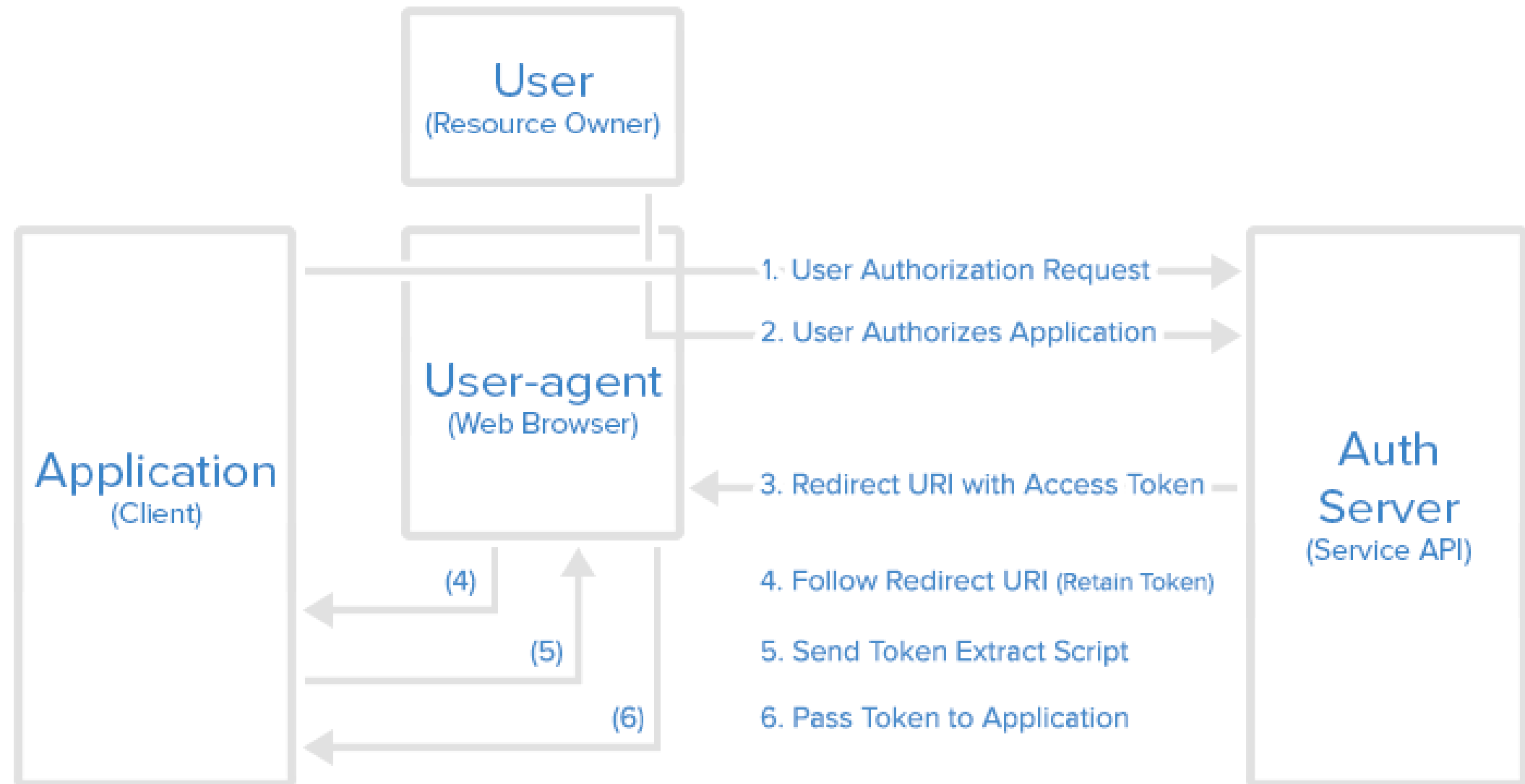
- 4. Application requests ACCESS_TOKEN

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

2. User Authorizes Application

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

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

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/facebook-login/access-tokens>