Google Cloud

Edge Security

OAuth - Authorization Code

OAuth grants

An OAuth Grant is a credential representing the resource owner's authorization. More often than not, we tend to think of grants in terms of the process used to obtain an access token.

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No
A specific resource owner is involved		
Resource Owner Password Credentials	Resources are owned by a particular user and the requesting application is trusted	A bit
Authorization Code	Resources are owned by a particular user and the requesting application is untrusted	Very
Implicit	Resources are owned by a particular user, and the requesting application is an untrusted browser-based app written in a scripting language such as JavaScript	Very, and potentially insecure as well

Authorization code grant type

Resources participating in authorization code grant type

- End user
- Client application
- User agent
- Edge - generating and validating token
- Authentication server - to validate the credentials
- Backend API resource

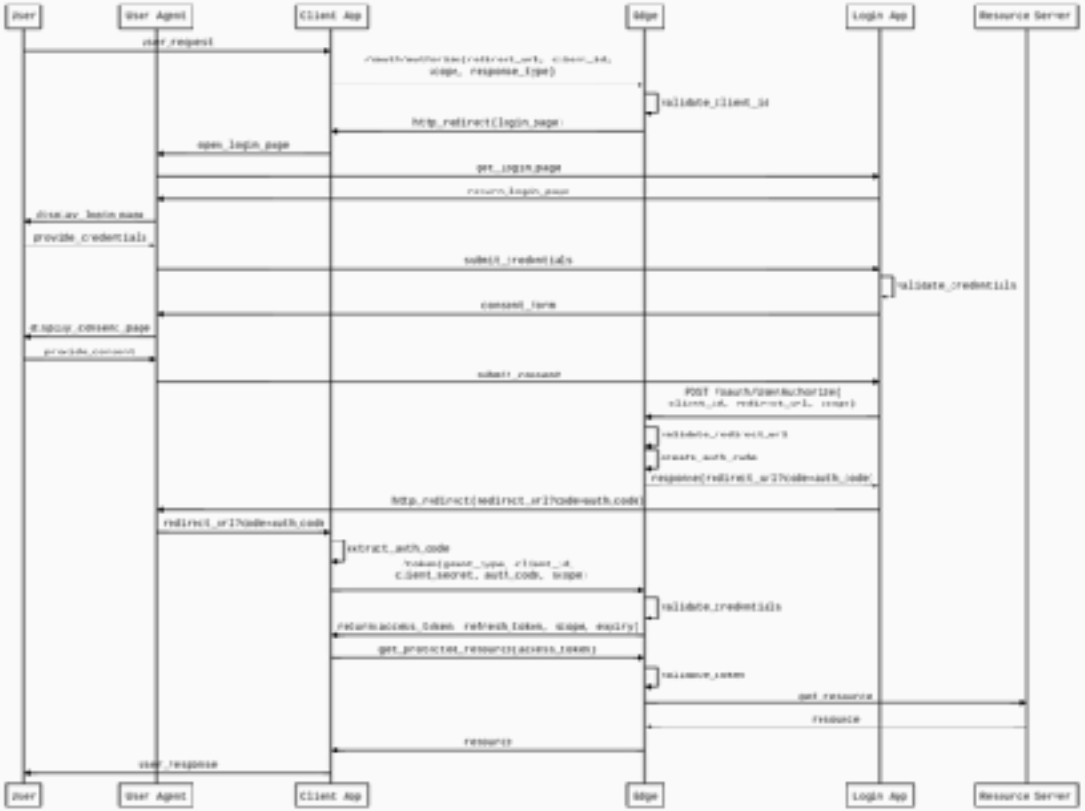
Resource owner is involved, typically owned by user and requesting application is untrusted

Very complex to implement compared to client credentials or password grant type

More secure than password grant type

Refresh token generated along with bearer token

Authorization code - Sequence diagram



Generate authorization code

```
<OAuthV2 async="false" continueOnError="false" enabled="true" name="GetAuthCode">
    <DisplayName>GetAuthCode</DisplayName>
    <Operation>GenerateAuthorizationCode</Operation>
    <ExpiresIn>600000</ExpiresIn>
    <GenerateResponse/>
</OAuthV2>
```

Exchange authorization code for access token

```
<OAuthV2 name="GetAccessToken">
    <Operation>GenerateAccessToken</Operation>
    <ExpiresIn>360000000</ExpiresIn>
    <SupportedGrantTypes>
        <GrantType>authorization_code</GrantType>
    </SupportedGrantTypes>
    <GrantType>request.queryparam.grant_type</GrantType>
    <GenerateResponse/>
</OAuthV2>
```

Verify OAuth token policy

The OAuthV2 policy's *VerifyAccessToken* operation will validate the access token for subsequent requests for all grant types.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<OAuthV2 async="false" continueOnError="false" enabled="true" name="VerifyOAuthToken">
    <DisplayName>OAuth Verify Token</DisplayName>
    <Operation>VerifyAccessToken</Operation>
</OAuthV2>
```

Set the access token as the bearer token in the authorization header of the http request.

```
curl -H "Authorization: Bearer {access_token}"
http://myorg-test.apigee.net/v1/cc/oauth_cc_weather/forecastrss?w=12797282
```

THANK YOU