

# Fullstack Development

# Authentication / Authorization

## **Part 2: Social signing up/in**

# Something like this

*We need OAuth 2.0.*



Sign in with Google



Sign in with Facebook



Sign in with Apple



Sign in with Twitter




Sign in with email

Part 2: Social signing up/in

## **Section 2A: OAuth 2.0**

# OAuth 2.0

## 3rdPartApp wants to access your Google Account

 some@email.com

This will allow 3rdPartApp to:

31

View and edit events on all your calendars



### Make sure you trust 3rdPartApp

You may be sharing sensitive info with this site or app. Learn about how calendly.com will handle your data by reviewing its [terms of service](#) and [privacy policies](#). You can always see or remove access in your [Google Account](#).

[Learn about the risks](#)

Cancel

Allow

# OAuth 2.0

- "Open Authorization"
- Standard designed to allow application to access resources hosted by other web apps on behalf of a user.
  - Standard for `author`
  - Not for `authn`
- Replaced OAuth 1.0 in 2012.

# OAuth 2.0

- Specifies many "flows"
  - **Authorization Code Flow**
  - Client Credentials Flow
  - Refresh Token Flow
  - JWT Bearer Flow
  - Device Code Flow
- We will use "Authorization Code Flow" for social login.



# Recommended resources

- <https://engineering.backmarket.com/oauth2-explained-with-cute-shapes-7eae51f20d38>
- [https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc?utm\\_source=pocket\\_shared](https://developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauth-and-oidc?utm_source=pocket_shared)
- <https://youtu.be/8aCyojTIW6U?si=YPxkcLPcAoK5jixl>
- <https://youtu.be/t18YB3xDfXI?si=pD1JnFP0GrnBXW2v>

# Wait

Are we using OAuth (standard for `author`) and **authorization** code flow for `authn`?

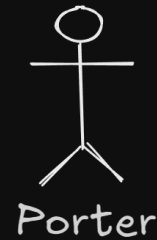
Yes, we kind of "misusing" it.

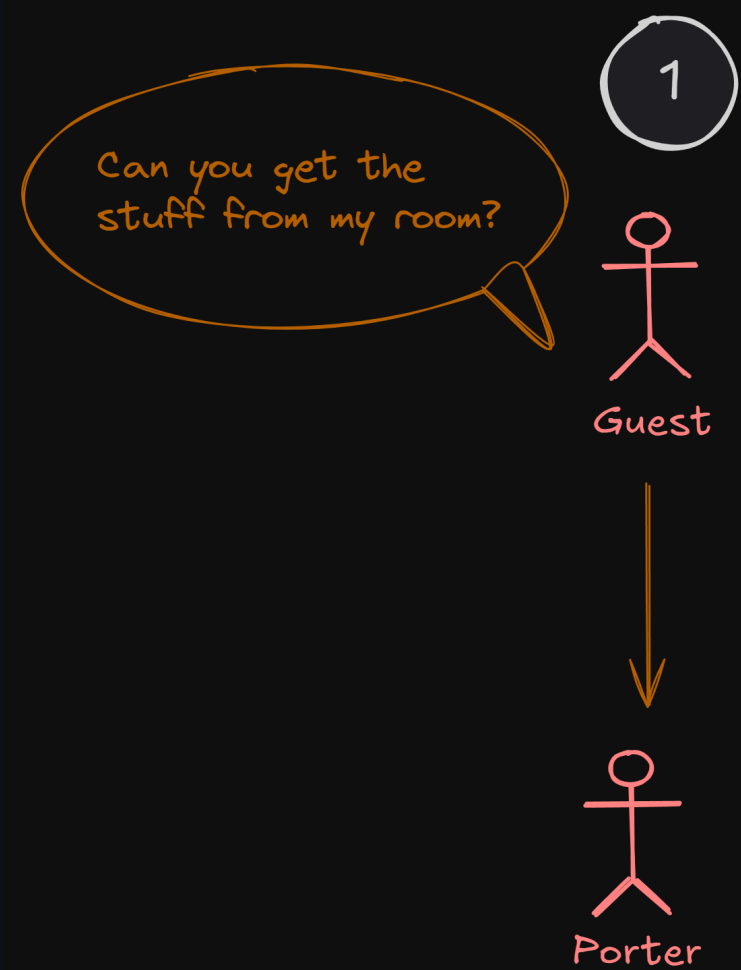
# Authorization code flow

| In real life

# Setup

- You are a guest at a hotel.
- You already checked out.
- You forgot your stuff in the room.
- You want a porter to get your stuff for you.



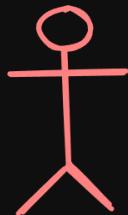


2

Sure, can you talk  
to receptionnist?



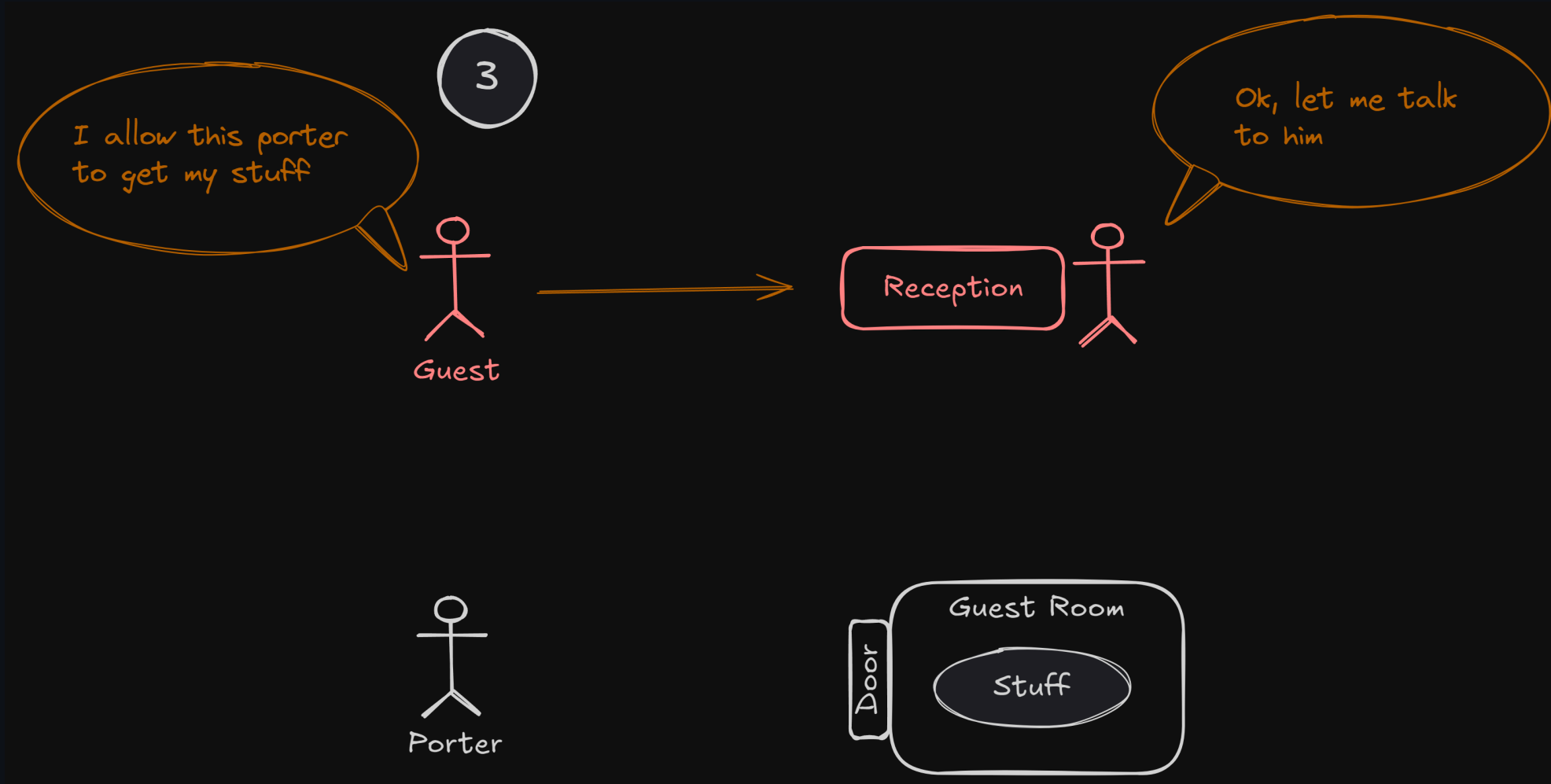
Guest

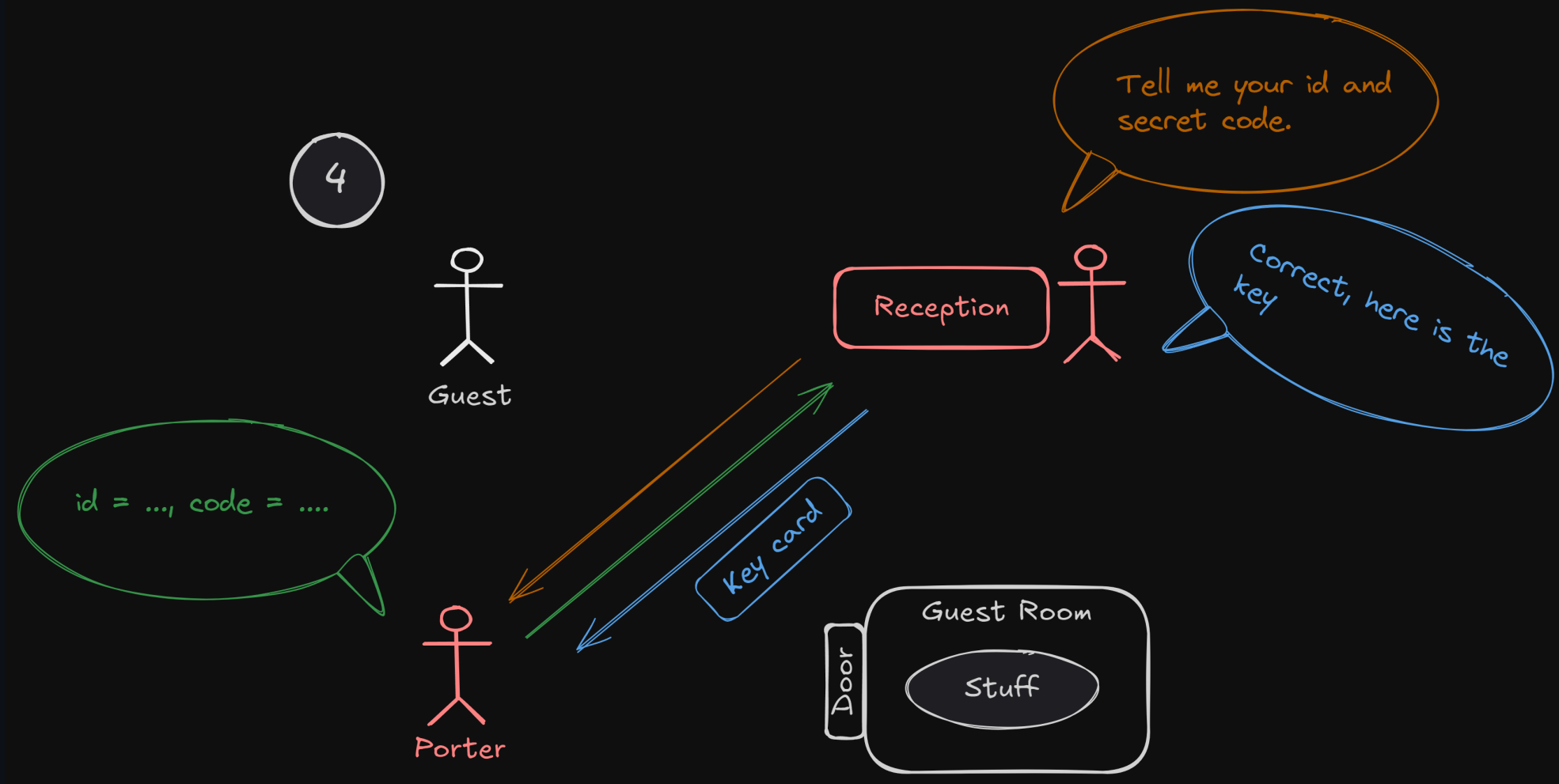


Porter

Reception









5



Guest

Reception



Porter

Key card

Door

Guest Room

Stuff

# Authorization code flow

- You ( `guest` ) authorize `porter` to access your resource.
- `porter` does not need to know who you are.
- The keycard reader at the door also doesn't need to have your information.

# Authentication?

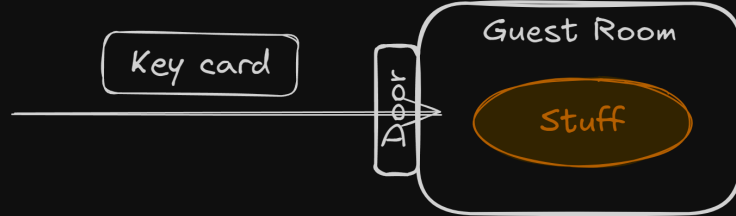
- But what if the porter wants to know who you are.
- There are two ways.

5 OAuth

Guest

Reception

Porter

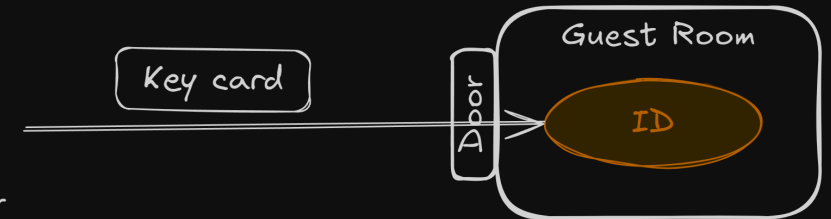


5 OAuth (Abused)

Guest

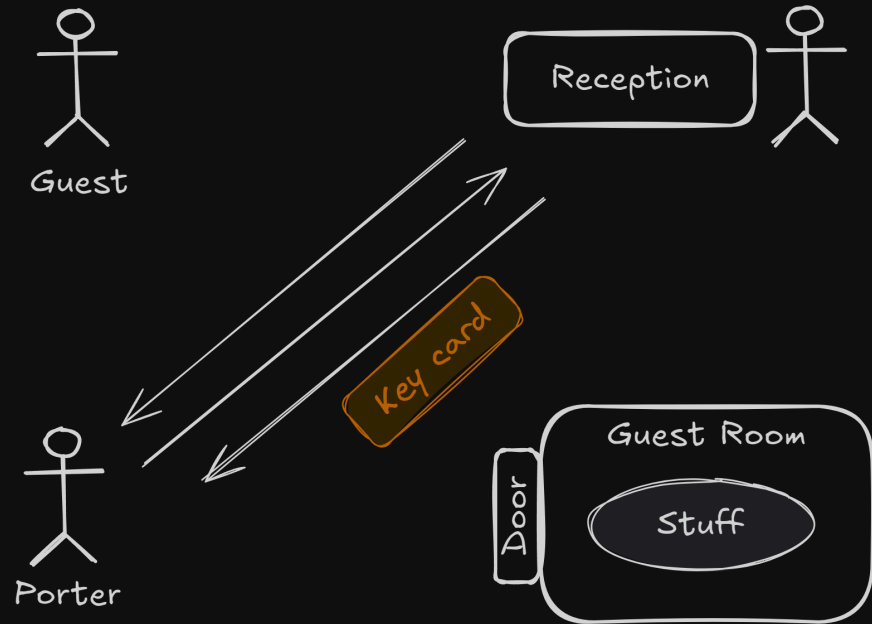
Reception

Porter

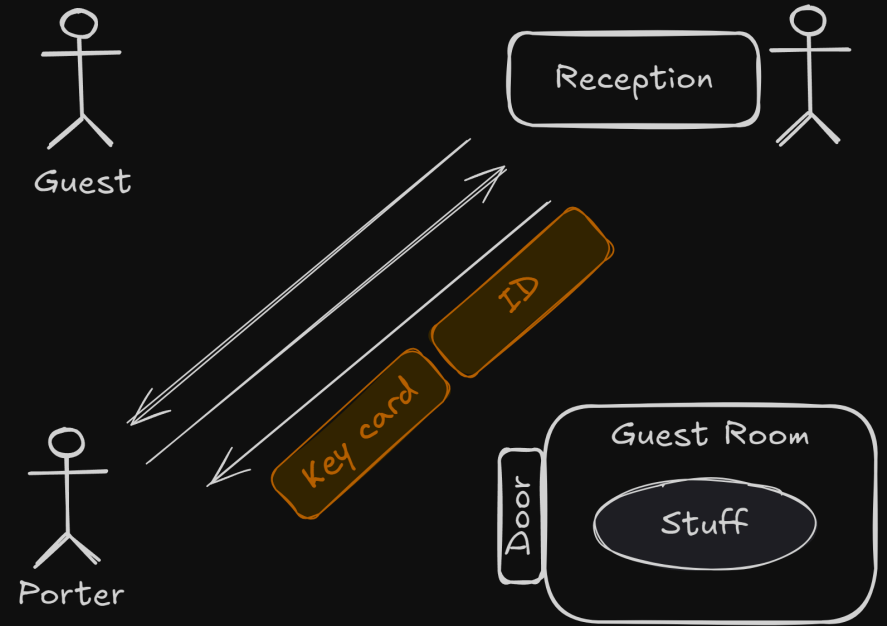


*This is what we are using.  
Is there a better way?*

#### 4 OAuth



#### 4 Open ID Connect



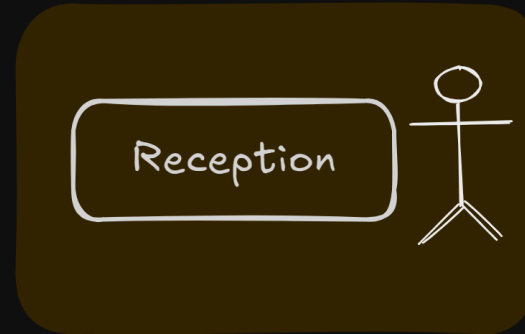
# OpenID Connect (OIDC)

- Thin layer that sits on top of OAuth 2.0
  - Adds login and profile information about the person who is logged in.
- When a "Authorization Server" supports OIDC, it is sometimes called an "Identity Provider".
- Not all servers support OIDC.

## Resource owner (user)



## Authorization server

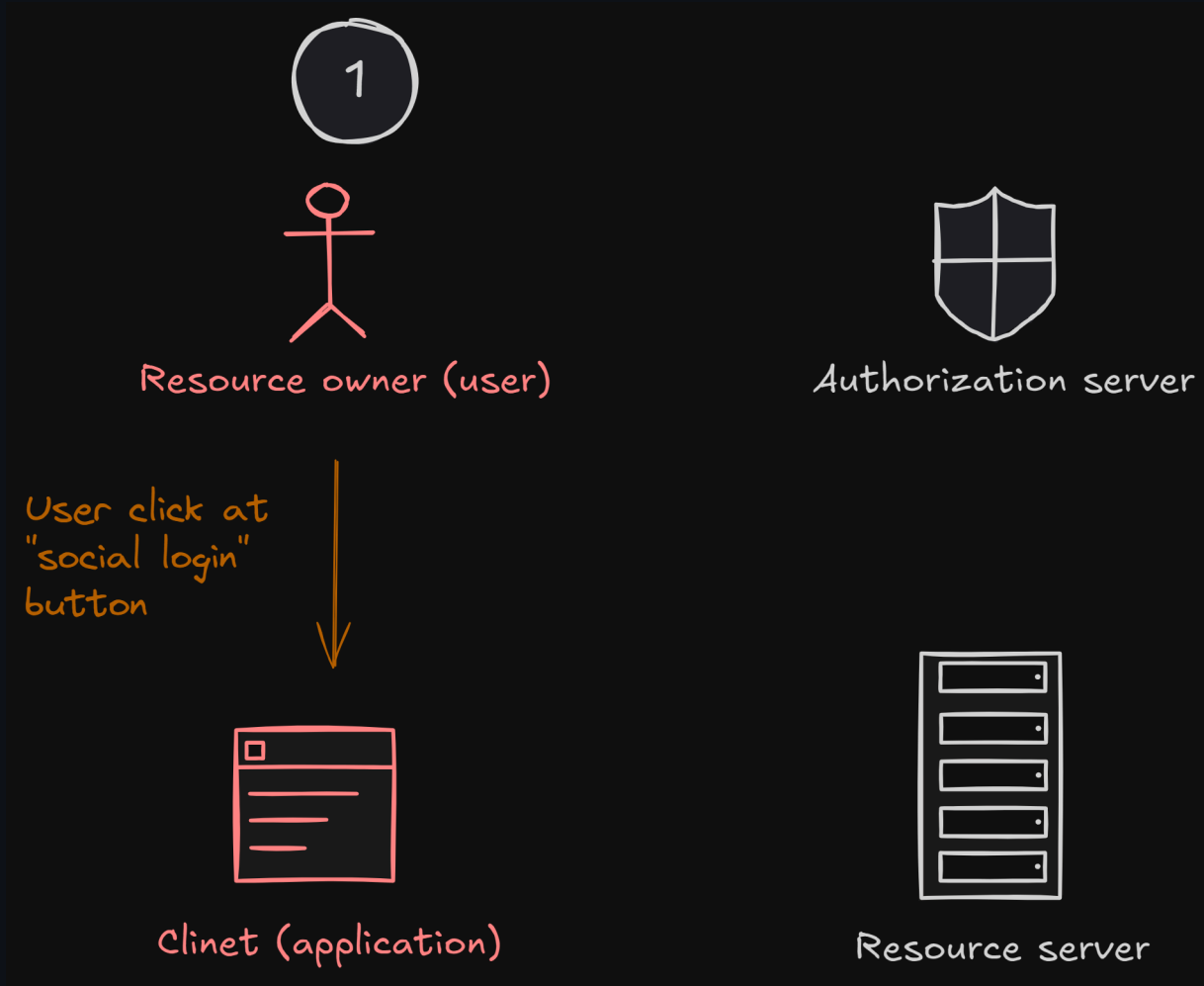


## Clinet (application)



## Resource server







2



Resource owner (user)



Authorization server

Client redirect user to  
"Authorization URL"



Client (application)

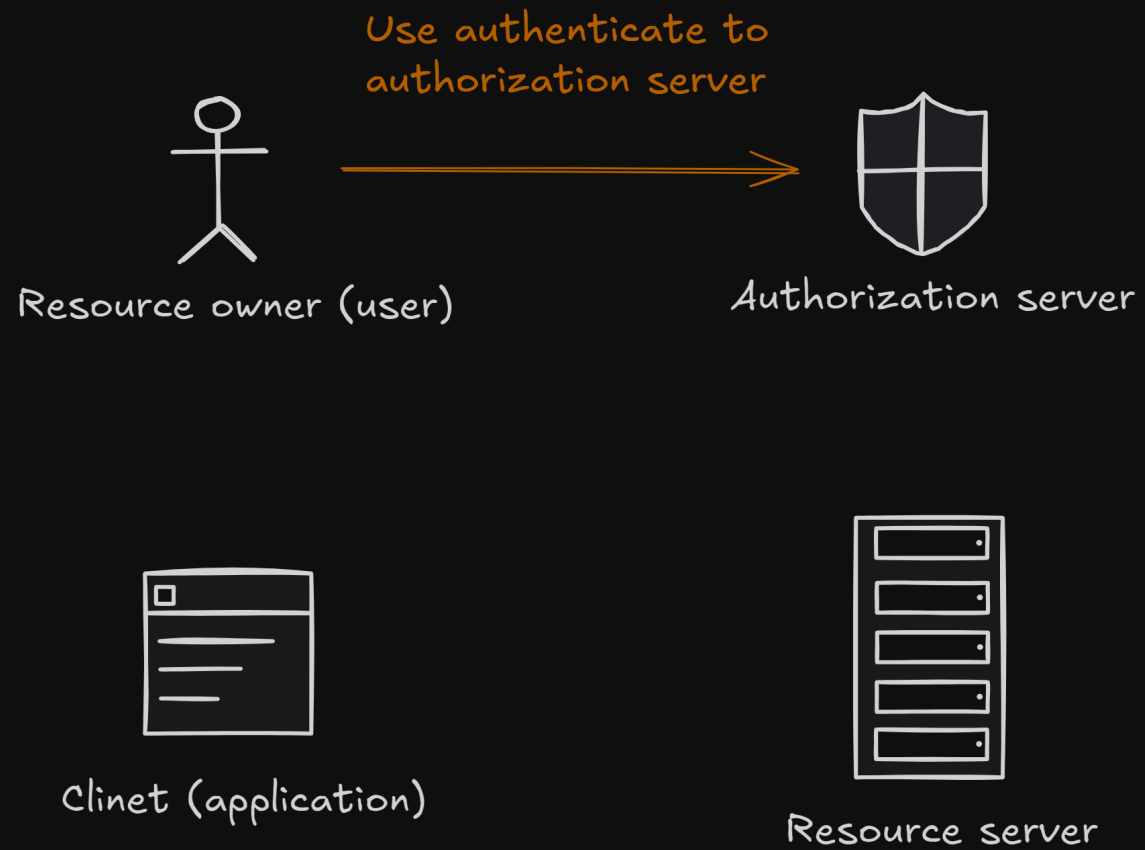


Resource server

Contains

- Client ID
- Scope
- Response type
- ...

3



44



Resource owner (user)



Authorization server

Authorization server  
invokes "callback url".

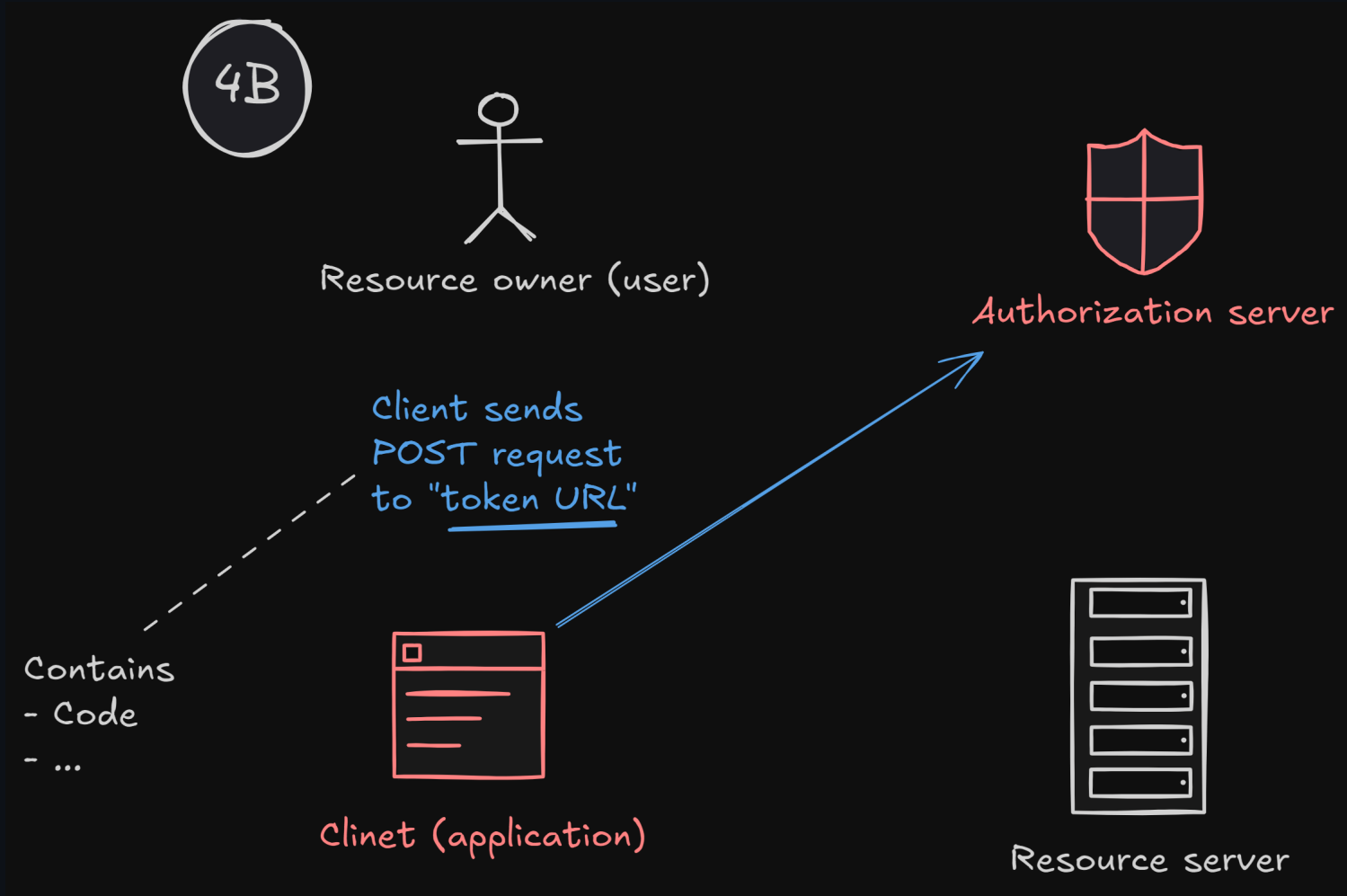
Contains  
- Code  
- ...



Client (application)



Resource server



4c



Resource owner (user)

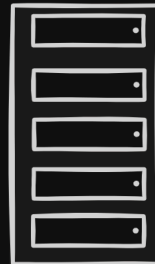


Authorization server

Authorization server  
response with  
"access token".

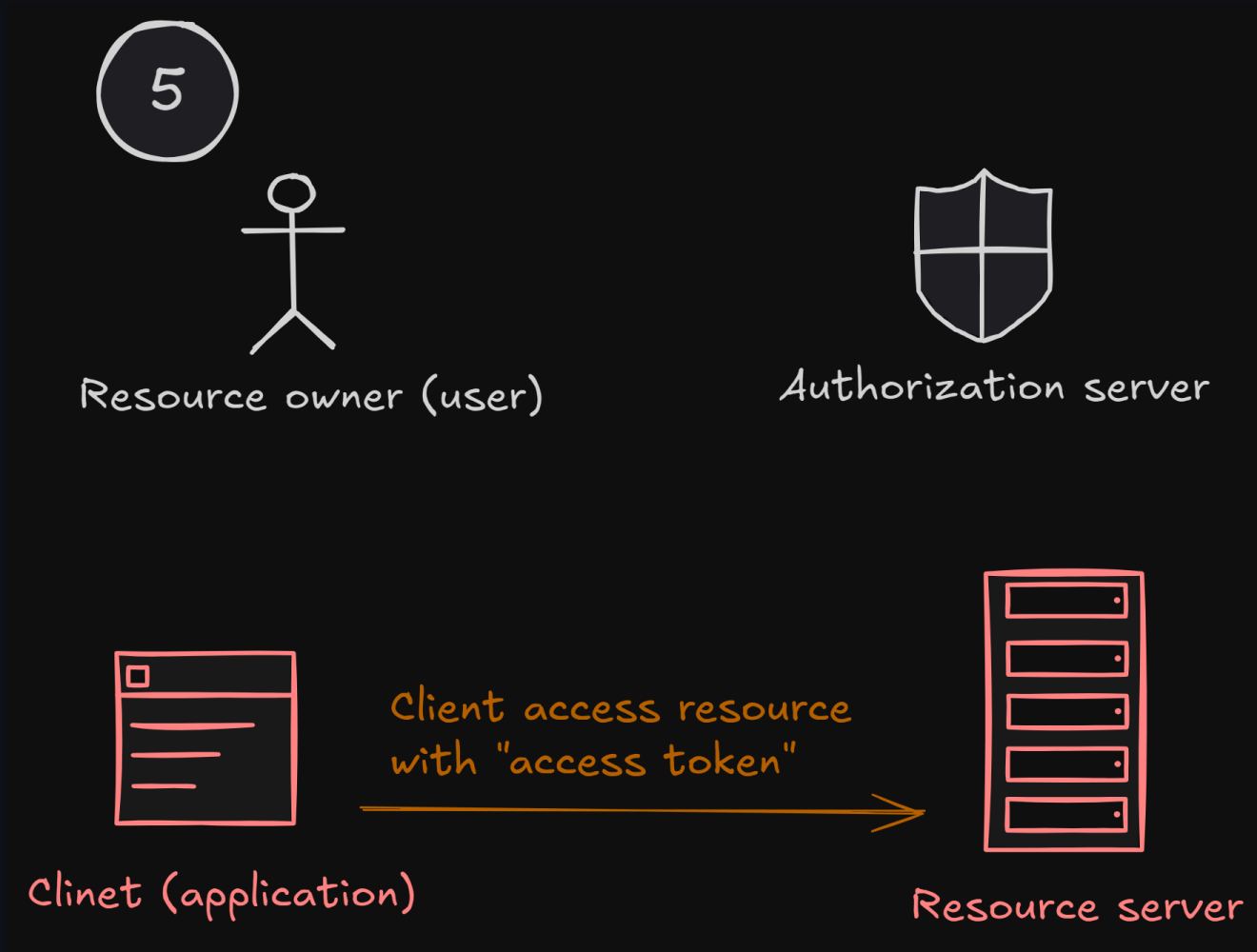


Client (application)



Resource server





Part 2: Social signing up/in

## **Section 2B: Oauth 2.0 with Github (Lab)**

# You will need

- Client ID = ...
- Client Secret = ...
- Callback URL = `http://localhost:5001/whatever`
- Authoriation URL = ...
- Token URL = ...
- Resource URL
  - `https://api.github.com/user`
  - `https://api.github.com/user/emails`
- Access Token = ...



# Setup

- Register your app [here](#).
- `Homepage URL` and `Callback URL` can be whatever for now.

## Register a new OAuth application

**Application name \***

fs-auth-2

Something users will recognize and trust.

**Homepage URL \***

http://localhost:5001

The full URL to your application homepage.

**Application description**

Application description is optional

This is displayed to all users of your application.

**Authorization callback URL \***

http://localhost:5001/whatever

Your application's callback URL. Read our [OAuth documentation](#) for more information.

☐ **Enable Device Flow**

Allow this OAuth App to authorize users via the Device Flow.

Read the [Device Flow documentation](#) for more information.

Register application

Cancel

# Setup

- Get Client ID and Client Secret

## fs-auth-2



nnnpooh owns this application.

Transfer ownership

You can list your application in the [GitHub Marketplace](#) so that other users can discover it.

List this application in the Marketplace

0 users

Revoke all user tokens

Client ID

0v231iwDq5jdIXDiQXI2

Client secrets

Generate a new client secret

Make sure to copy your new client secret now. You won't be able to see it again.



Client secret

✓ 23b7d193673020a537c62697312eb50a14353937

Added now by nnnpooh

Never used

You cannot delete the only client secret. Generate a new client secret first.

Delete

# Setup

- Choose `scope`.
  - `scope=user,user:email`
- Construct Authorization URL
  - `https://github.com/login/oauth/authorize?client_id=CLIENT_ID&redirect_uri=REDIRECT_URL&response_type=code&scope=SCOPE`

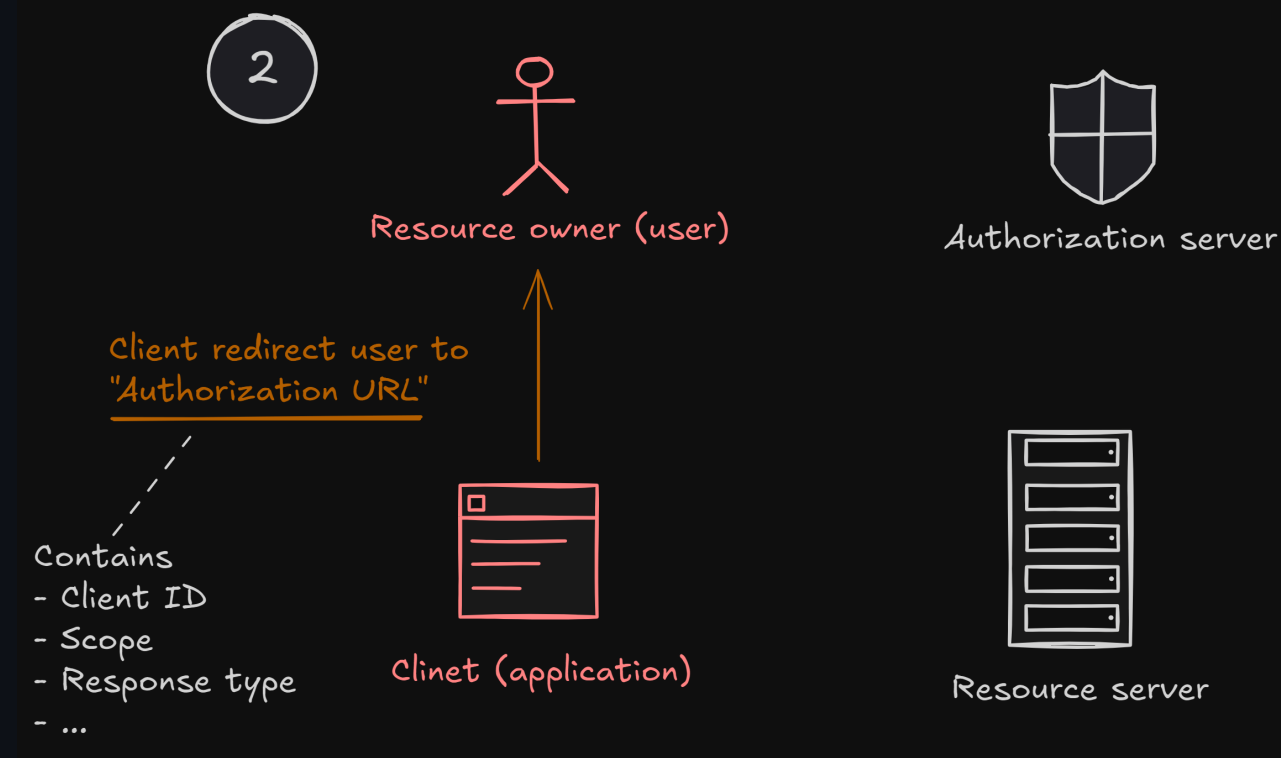
# Setup

- Construct Token URL (*incompleted*)
  - `https://github.com/login/oauth/access_token?`  
`client_id=CLIENT_ID&client_secret=CLIENT_SECRET&code=CODE&redirect_uri=CAL`  
`LBACK_URL`

**Let's go**

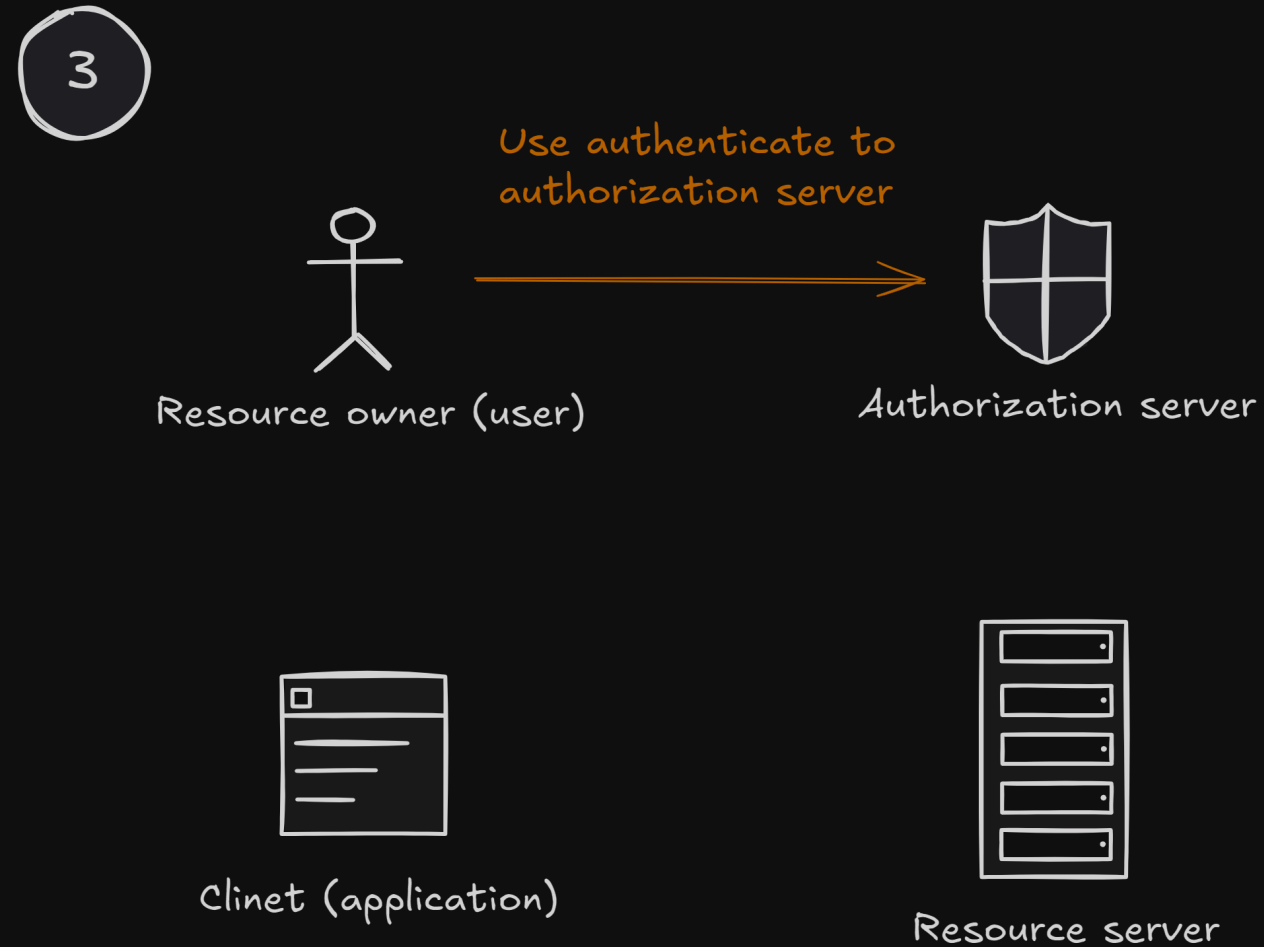
## Step 2

- *(Skip 1 for now since there is no app.)*
- Goto at **Authorization URL**



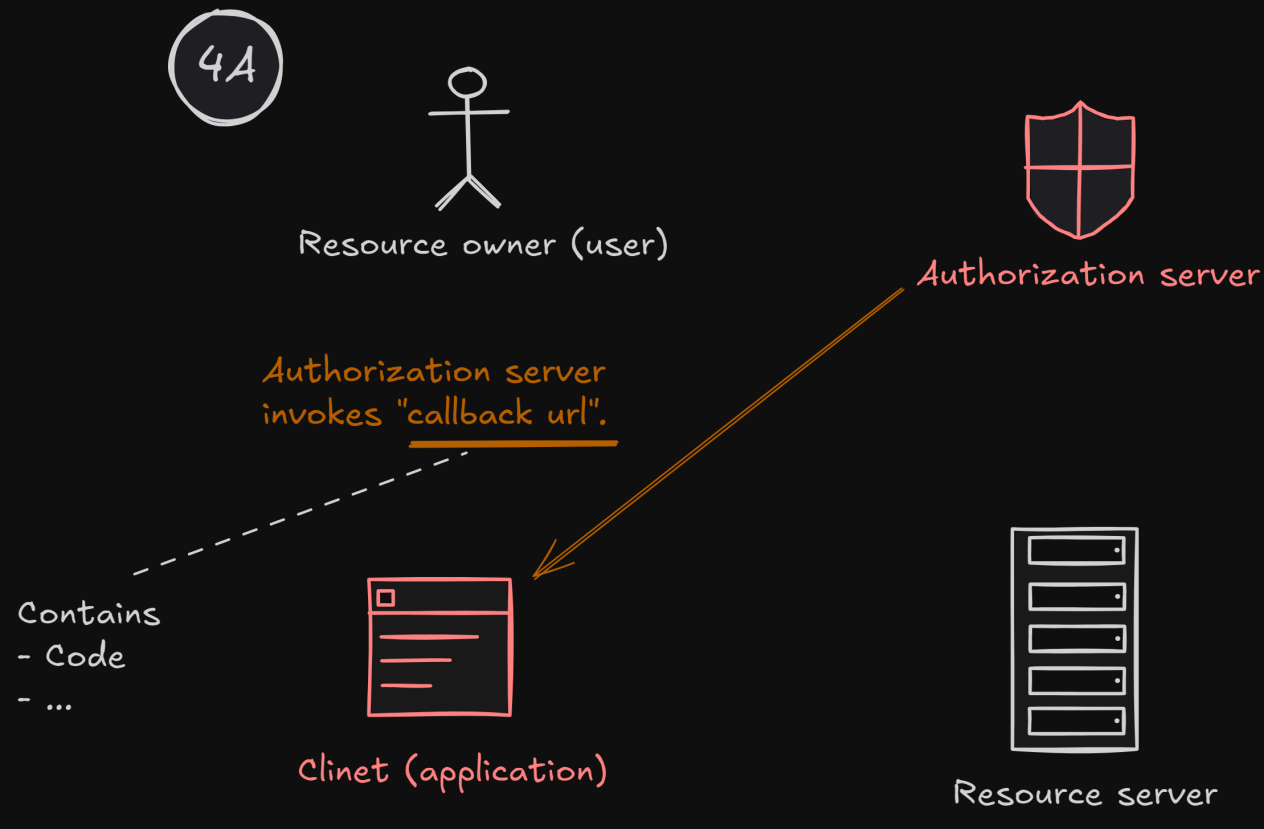
## Step 3

- Authenticate with Github



## Step 4A

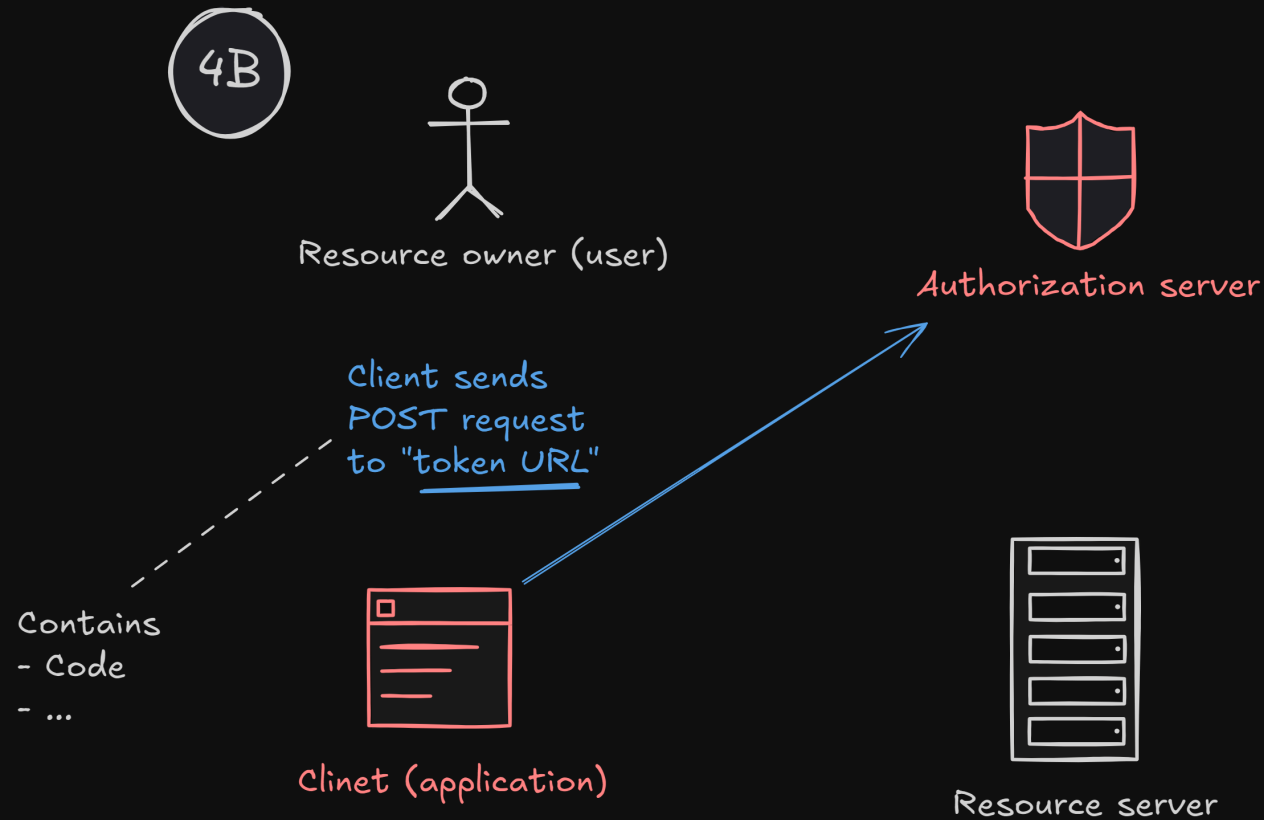
- Extract `code` and keep it.
- `code` is usually very short-lived.





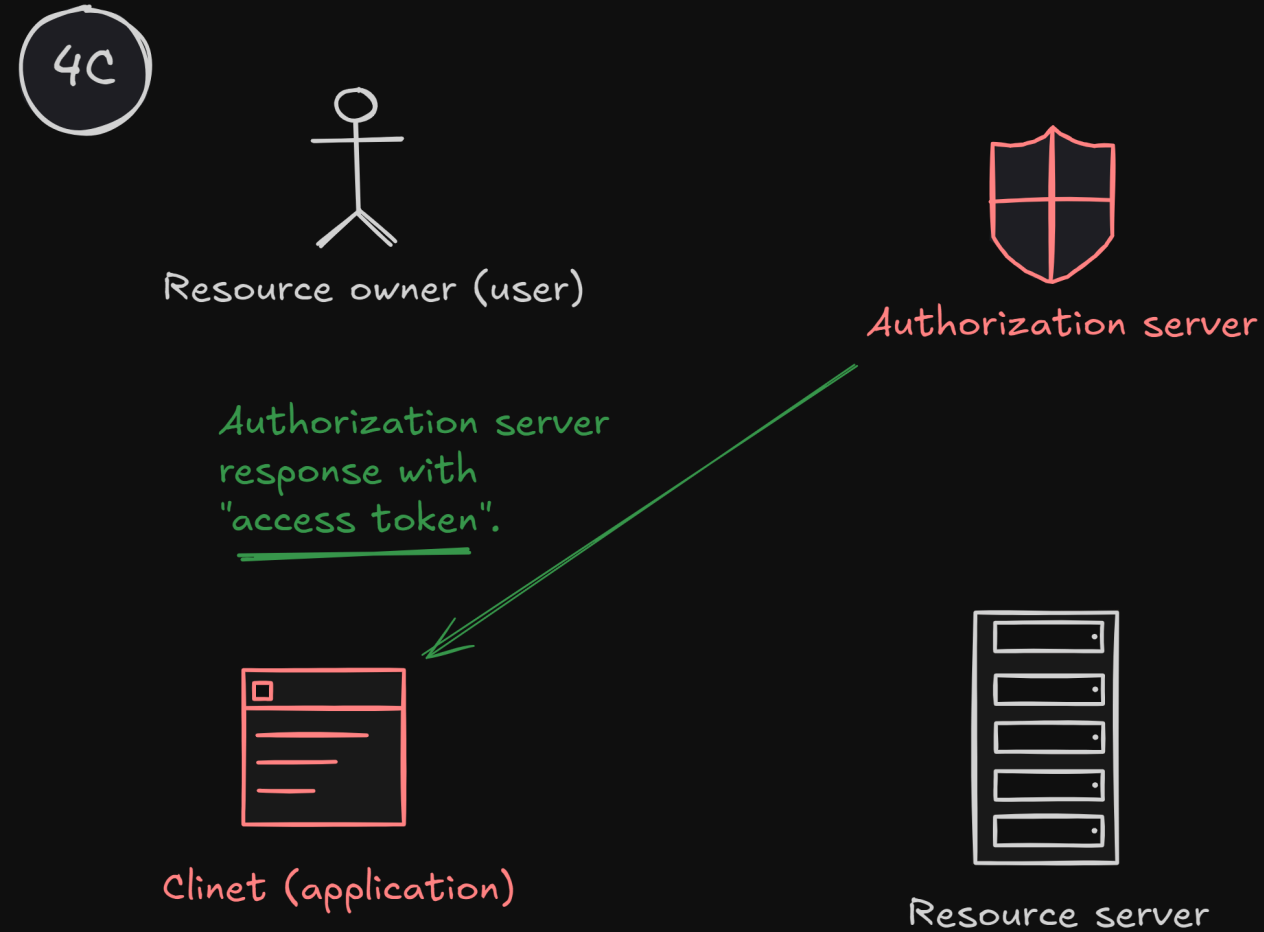
## Step 4B

- Send `POST` request to `Token URL` with actual `Code`.
- [Reference](#)



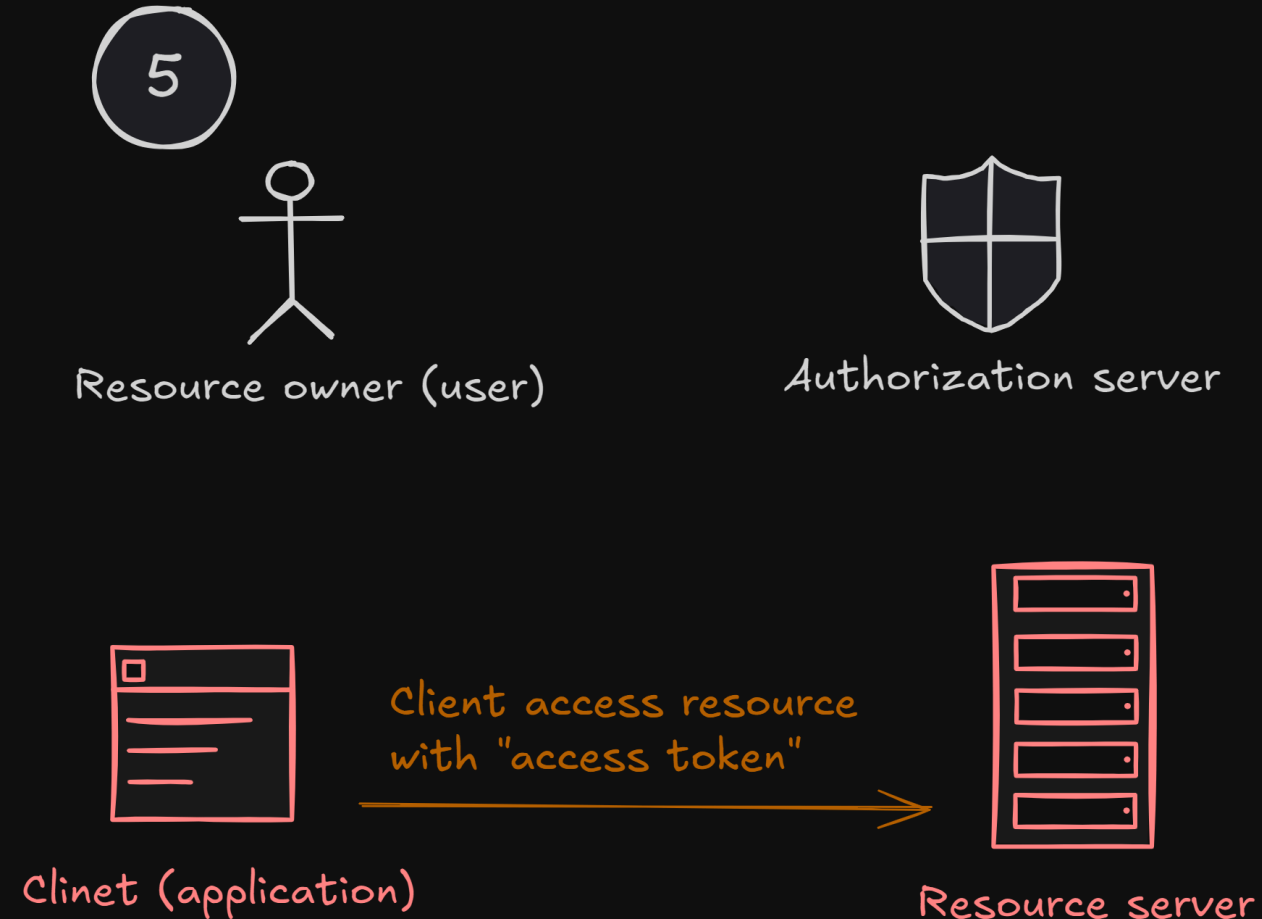
## Step 4C

- Keep **Access Token** from the response.



## Step 5

- Send **GET** request to resources.
- Use **Access Token** as bearer token.
- [Reference](#)



Search... Ctrl + P

Invite nnnpooh@gmail.com

Auth GET https://api.github.com/user Send 200 OK 491 ms 1421 B 5 Minutes Ago

Base Environment Add Cookies Add Certificates

Filter GET New Request POST New Request

URL PREVIEW https://api.github.com/user

Params Body Auth Headers 3 Scripts Docs

QUERY PARAMETERS

name	value
------	-------

PATH PARAMETERS

Path parameters are url path segments that start with a colon ':' e.g. 'id'

Preview

```
12 "starred_url":  
13 "https://api.github.com/users/nnnpoooh/starred{/owner}/{/repo}",  
14 "subscriptions_url":  
15 "https://api.github.com/users/nnnpoooh/subscriptions",  
16 "organizations_url":  
17 "https://api.github.com/users/nnnpoooh/orgs",  
18 "repos_url": "https://api.github.com/users/nnnpoooh/repos",  
19 "events_url":  
20 "https://api.github.com/users/nnnpoooh/events{/privacy}",  
21 "received_events_url":  
22 "https://api.github.com/users/nnnpoooh/received_events",  
23 "type": "User",  
24 "site_admin": false,  
25 "name": "Nirand",  
26 "company": "Chiang Mai University",  
27 "blog": "",  
28 "location": "Thailand",  
29 "email": null,  
30 "hireable": null,  
31 "bio": null,  
32 "twitter_username": null,  
33 "notification_email": null,  
34 "public_repos": 49,  
35 "public_gists": 32,  
36 "followers": 6,  
37 "following": 0,  
38 "created_at": "2019-10-05T05:21:33Z".
```

\$.store.books[\*].author

master

Preferences

Online Made with ❤ by Kong

# Google OAuth 2.0

- Authorization URL = `https://accounts.google.com/o/oauth2/v2/auth?client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&response_type=code&scope=openid+https://www.googleapis.com/auth/userinfo.email+https://www.googleapis.com/auth/userinfo.profile`
- Token URL = `https://oauth2.googleapis.com/token?client_id=CLIENT_ID&client_secret=CLIENT_SECRET&code=CODE&redirect_uri=CALLBACK_URL&grant_type=authorization_code`
- Resource URL = `https://www.googleapis.com/oauth2/v2/userinfo`

- ```
id_token .
```

# JSON Web Token

Part 2: Social signing up/in

## Section 2C: passport implementation

# Setup

- `git clone -b signin-oauth https://github.com/fullstack-67/auth-mpa-v2.git`  
`auth-signin-oauth`
- `pnpm i`
- `npm run db:reset`
- `npm run dev`



# Note

- Database tables
- Types of response objects
- Add type definition to `req.user`.

# Highlighted packages

```
{  
  "passport": "^0.7.0",  
  "passport-oauth2": "^1.8.0"  
}
```

```
// * Passport
passport.use("github", github);
passport.use("google", google);
app.use(passport.initialize());
```

```
export const github = new OAuthStrategy(  
  {  
    // Option  
  },  
  async function (  
    accessToken: string,  
    refreshToken: string,  
    profile: any,  
    done: VerifyCallback  
  ) {  
    // Do something with accessToken  
  }  
);
```