OAuth 2.0 introduction

Theory and code examples with Spring Boot

$ whoami

Nemanja Vasic

https://github.com/GoodbyePlanet

Topics

What is OAuth 2.0, and what problems does it solve

How it works, and what is it good for

OAuth 2.0 basic concepts

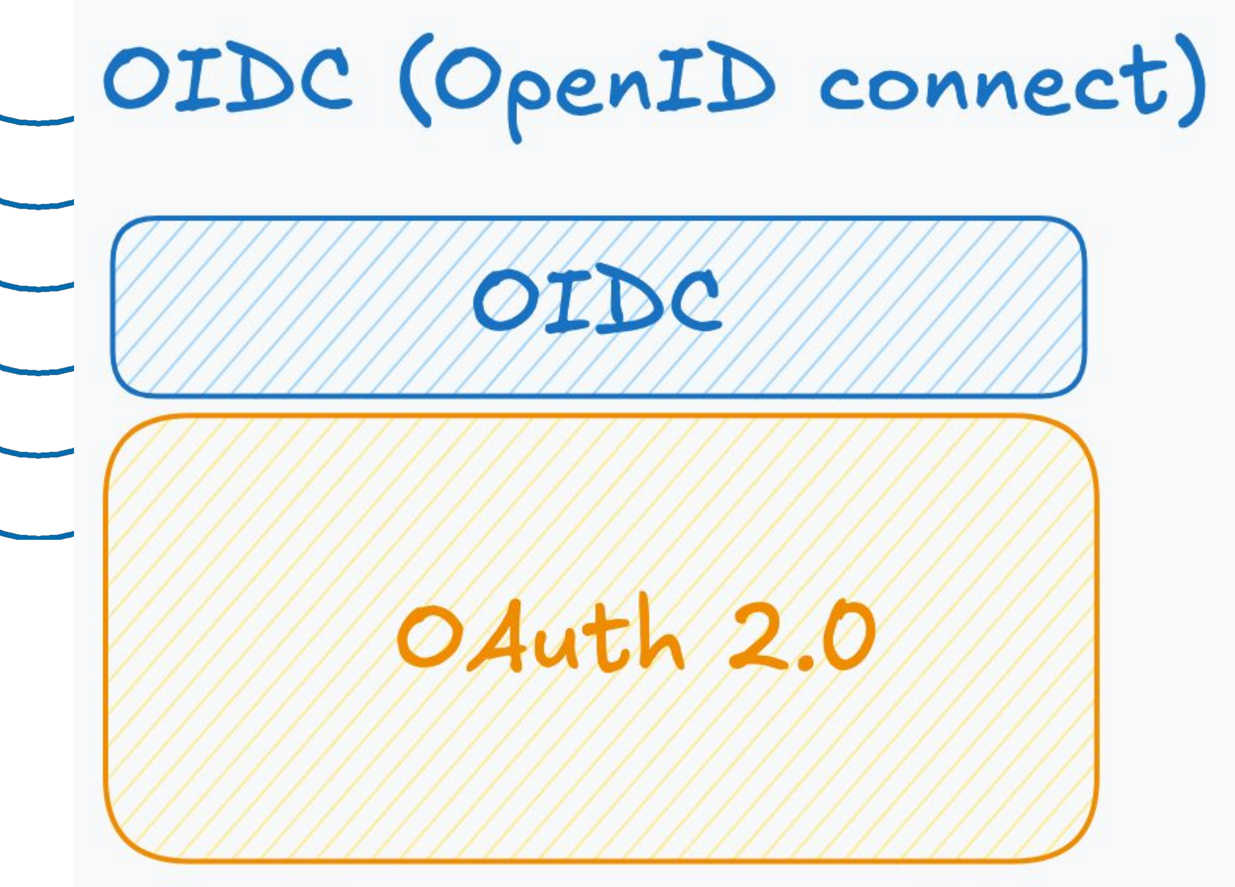
Basic OAuth 2.0 flows for redeeming an access token - examples

Code examples

What is OAuth 2.0?

What is delegated authorization problem?

Authorization vs Authentication



OIDC (OpenID connect)

OIDC

OAuth 2.0

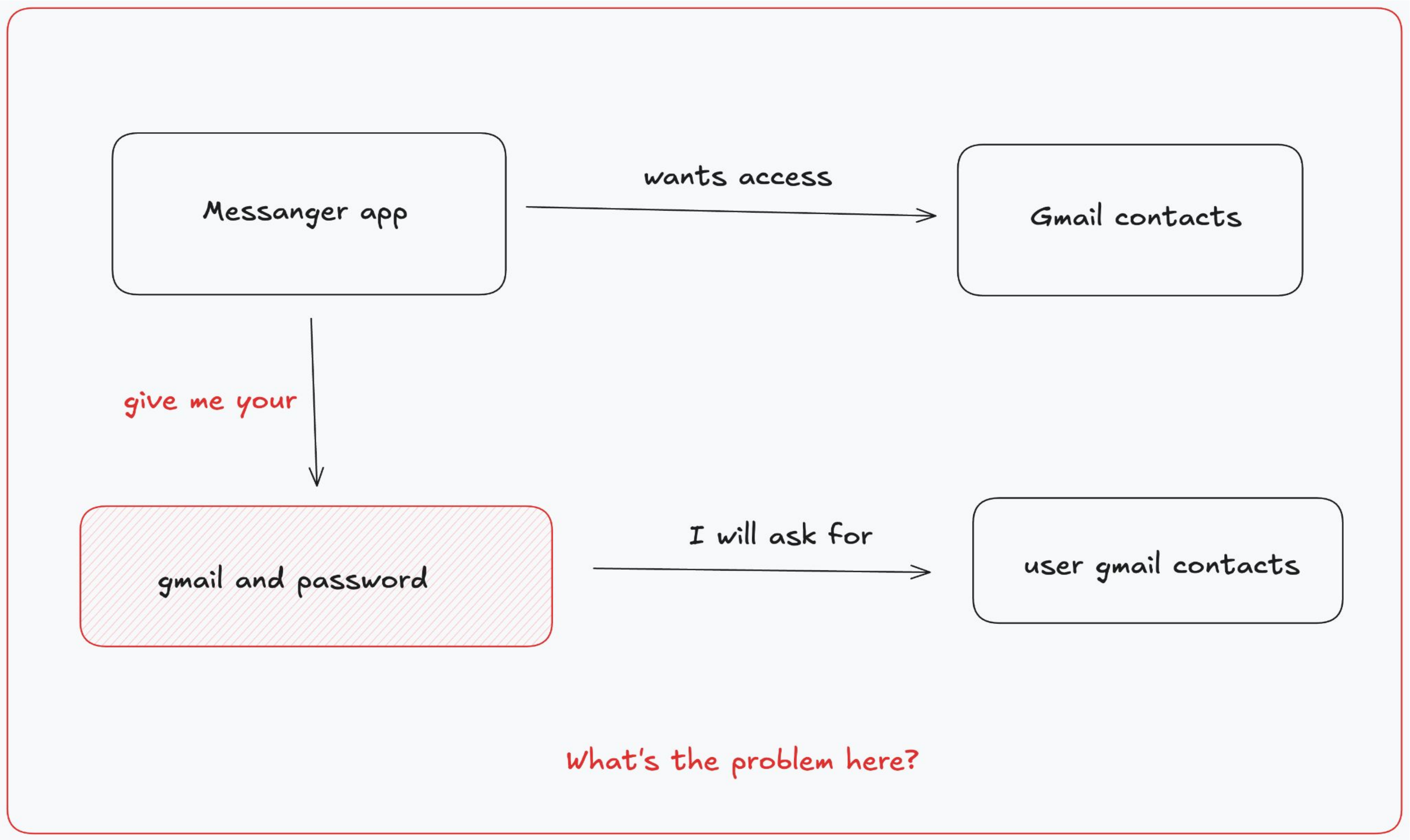
OAuth 2.0

- getting access to API
- getting access to user data present in other systems

OIDC

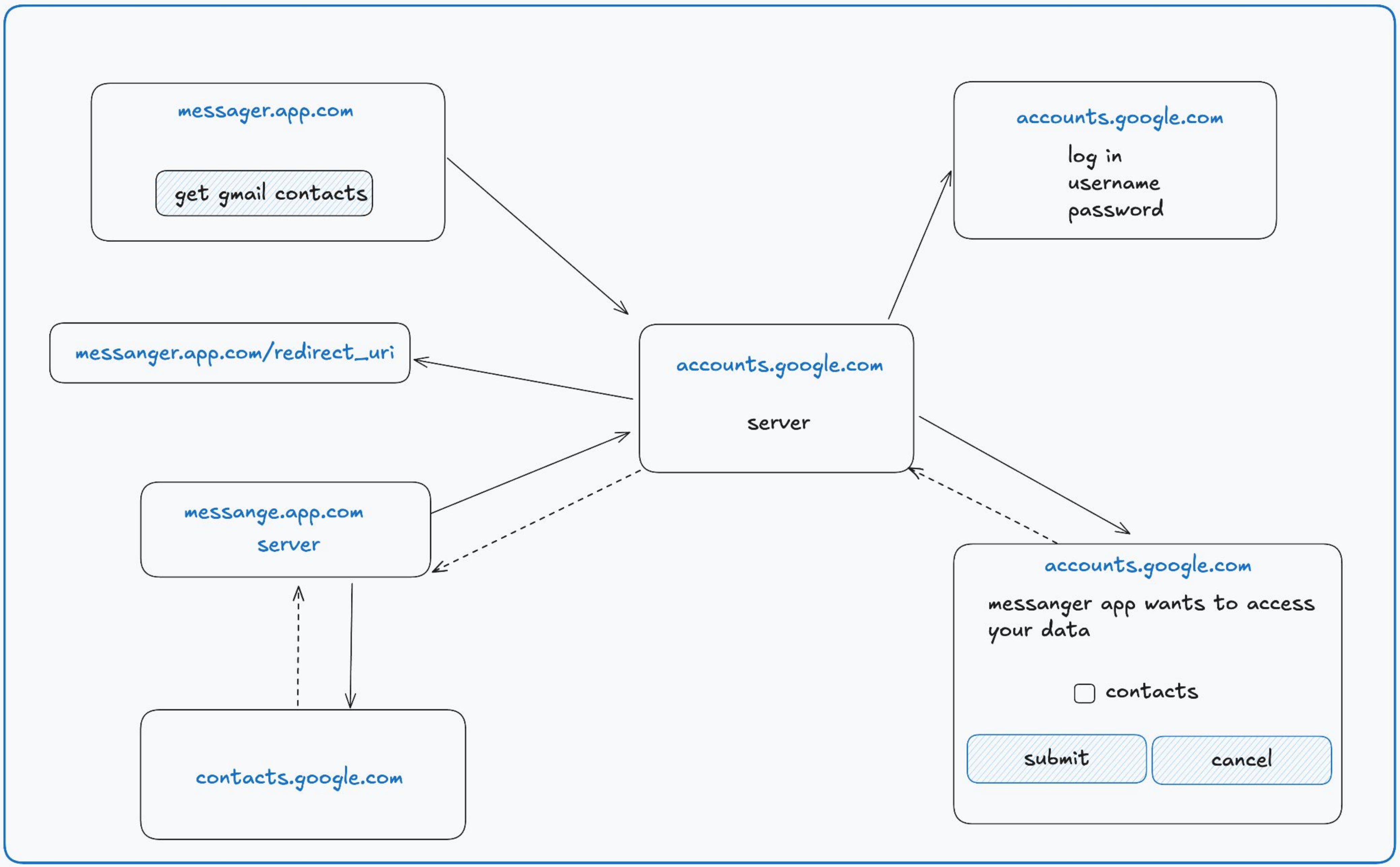
- logging user
- getting user details
- making user details available in other systems

Before OAuth 2.0



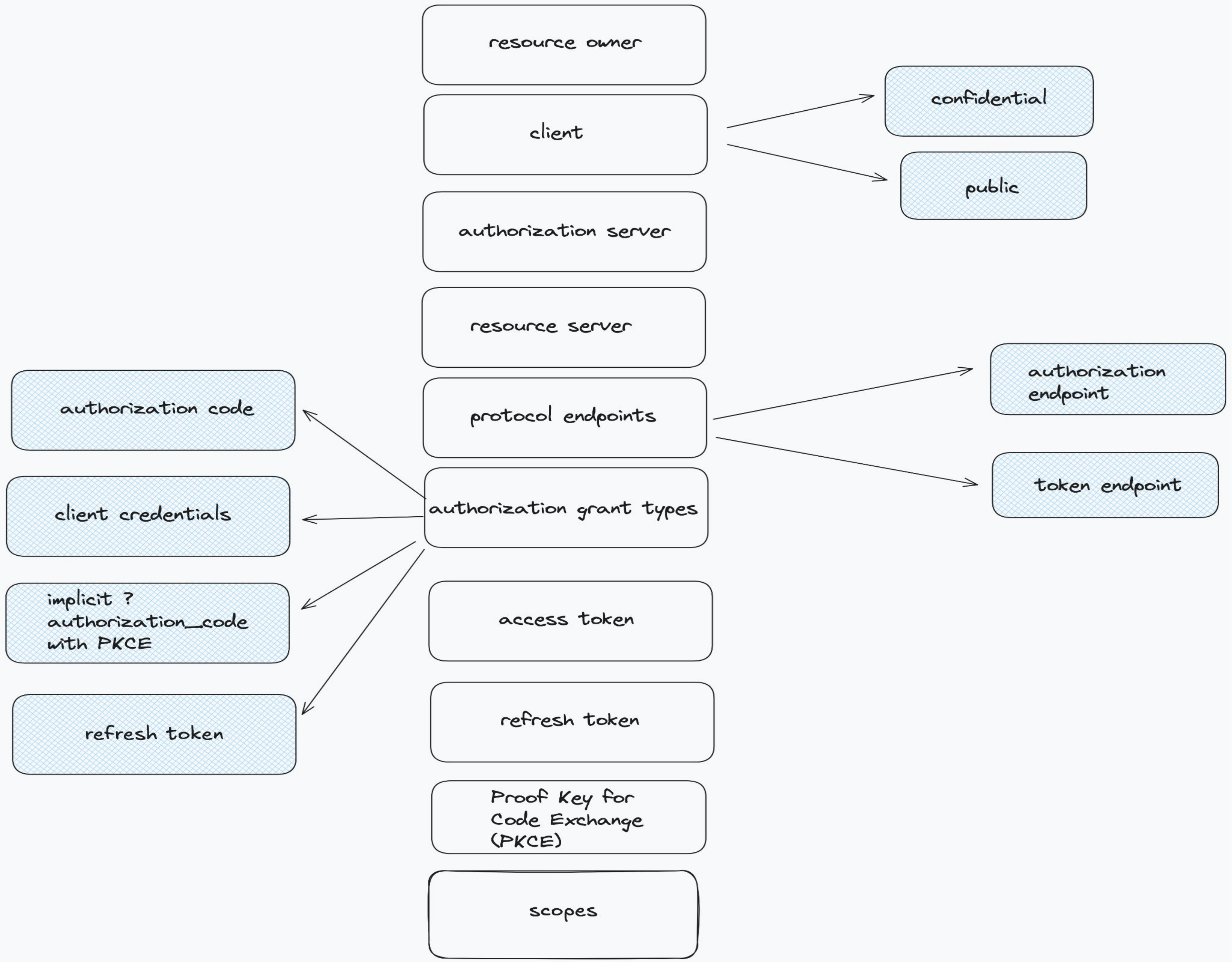
What's the problem here?

How it works with OAuth 2.0

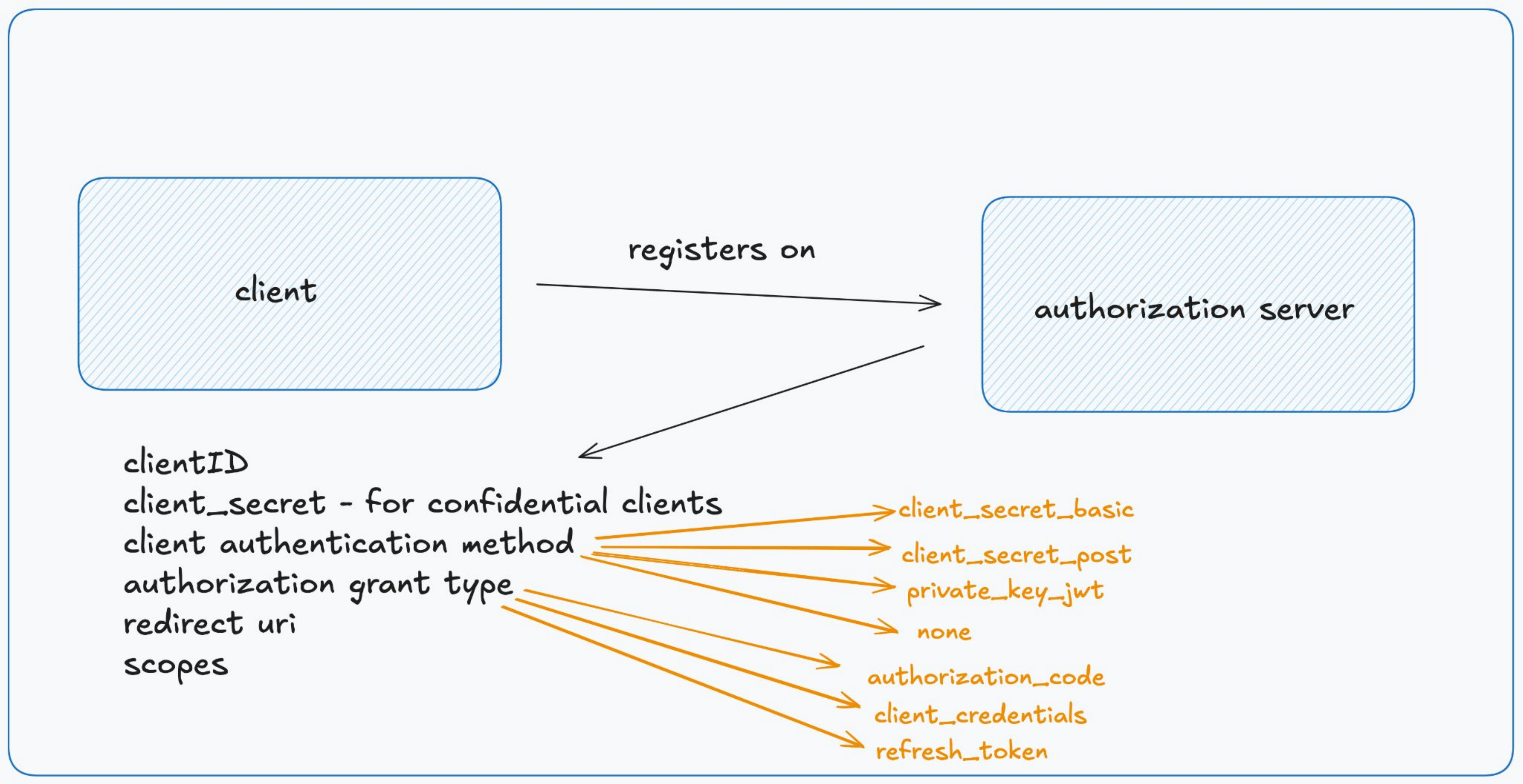


CORE CONCEPTS (ROLES)

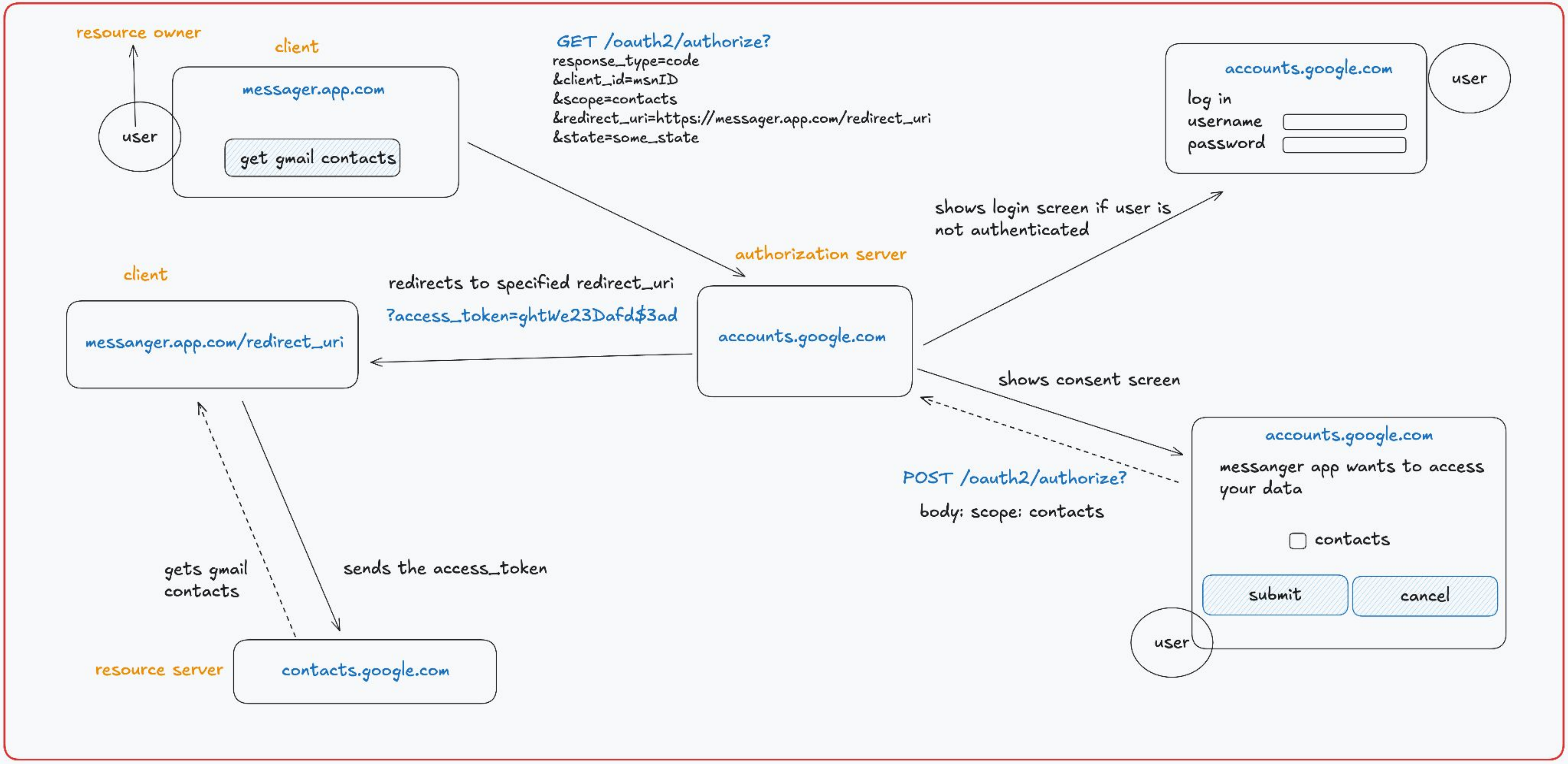
https://datatracker.ietf.org/doc/html/rfc6749#section-1.1



Client registration on Authorization Server



IMPLICIT Flow for PUBLIC client - Deprecated



resource owner

client

user

messager.app.com

get gmail contacts

GET /oauth2/authorize?
response_type=code
&client_id=msnID
&scope=contacts
&redirect_uri=https://messager.app.com/redirect_uri
&state=some_state

accounts.google.com

log in

username

password

user

shows login screen if user is not authenticated

authorization server

accounts.google.com

client

messanger.app.com/redirect_uri

redirects to specified redirect_uri

?access_token=ghtWe23Dafd$3ad

shows consent screen

POST /oauth2/authorize?

body: scope: contacts

accounts.google.com

messanger app wants to access your data

□ contacts

submit

cancel

user

gets gmail contacts

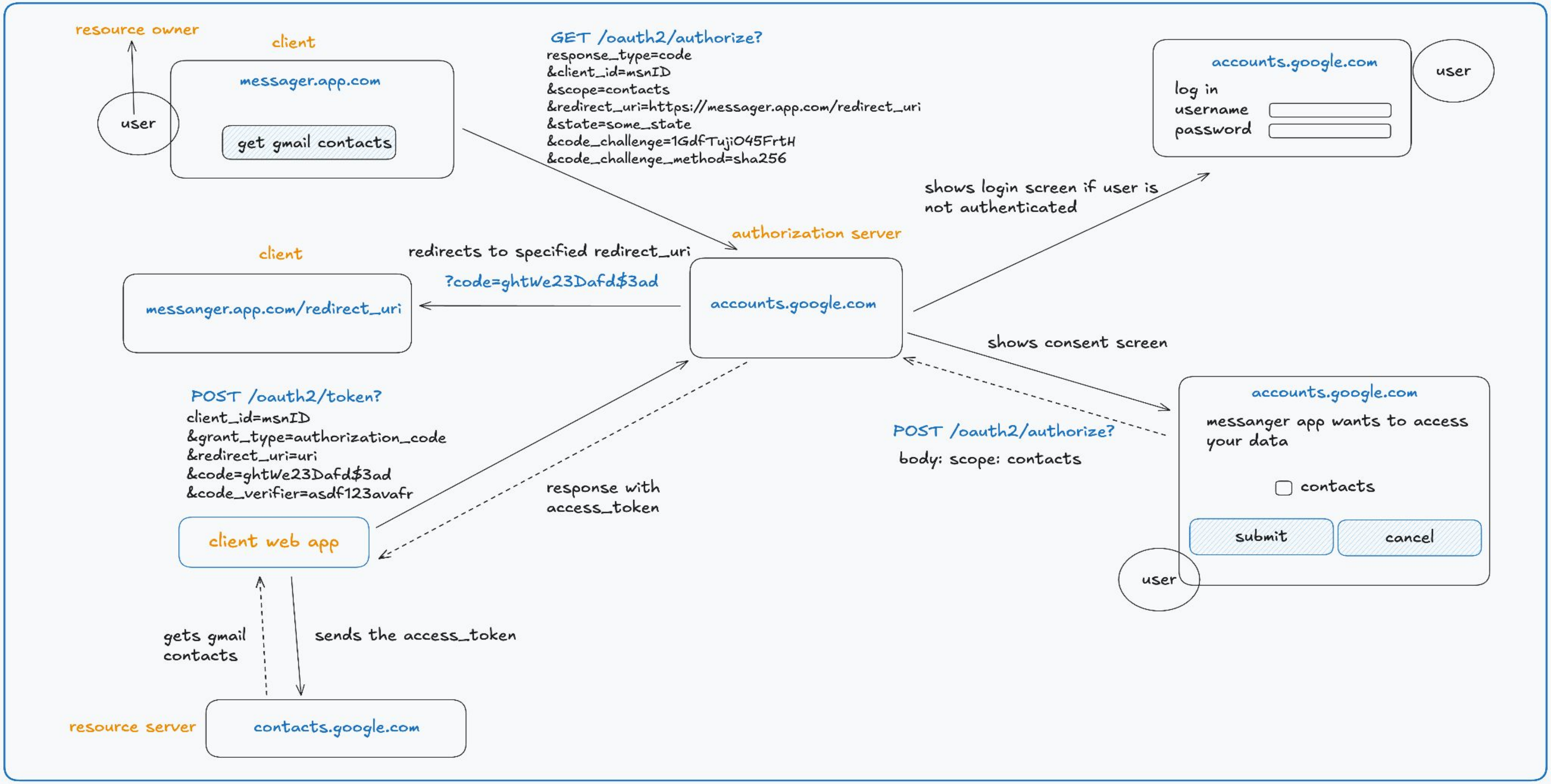
sends the access_token

resource server

contacts.google.com

https://developer.okta.com/blog/2019/05/01/is-the-oauth-implicit-flow-dead

Authorization code flow with PKCE (Proof Key for Code Exchange) - Recommended approach



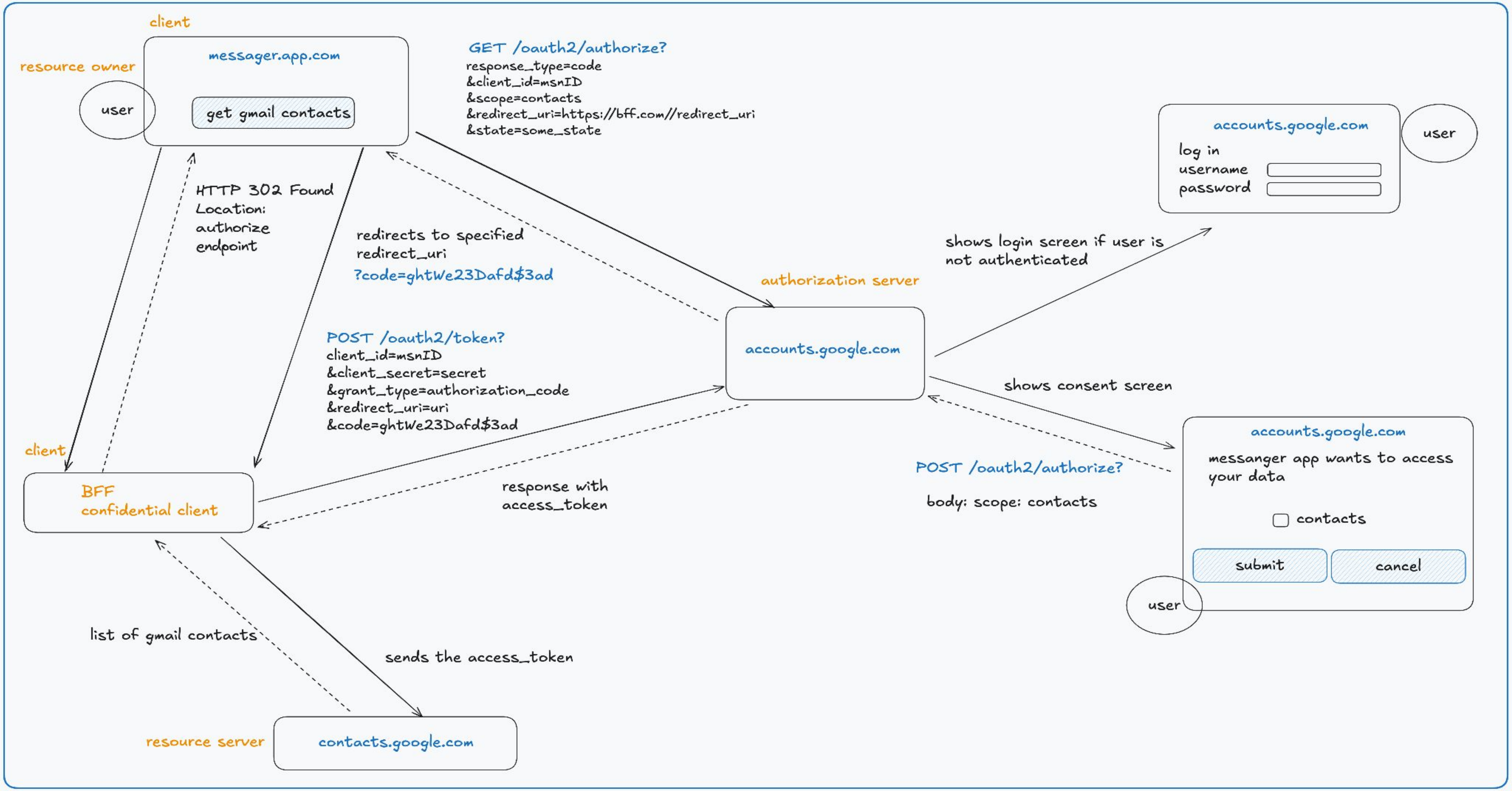
```
GET /oauth2/authorize?
response_type=code
&client_id=msnID
&scope=contacts
&redirect_uri=https://messager.app.com/redirect_uri
&state=some_state
&code_challenge=1GdfTuji045FrtH
&code_challenge_method=sha256
```

```
POST /oauth2/token?
client_id=msnID
&grant_type=authorization_code
&redirect_uri=uri
&code=ghtWe23Dafd$3ad
&code_verifier=asdf123avafr
```

```
POST /oauth2/authorize?
body: scope: contacts
```

https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow-with-pkce
https://github.com/spring-projects/spring-authorization-server/issues/297#issue-896744390

Authorization code flow with Confidential client (BFF approach) - Current best practice



client

resource owner

user

messager.app.com

get gmail contacts

GET /oauth2/authorize?
response_type=code
&client_id=msnID
&scope=contacts
&redirect_uri=https://bff.com//redirect_uri
&state=some_state

HTTP 302 Found
Location:
authorize
endpoint

redirects to specified
redirect_uri
?code=ghtWe23Dafd$3ad

accounts.google.com

user

log in
username
password

shows login screen if user is
not authenticated

authorization server

accounts.google.com

POST /oauth2/token?
client_id=msnID
&client_secret=secret
&grant_type=authorization_code
&redirect_uri=uri
&code=ghtWe23Dafd$3ad

shows consent screen

accounts.google.com

messanger app wants to access
your data

☐ contacts

submit

cancel

user

POST /oauth2/authorize?

body: scope: contacts

client

BFF
confidential client

response with
access_token

list of gmail contacts

sends the access_token

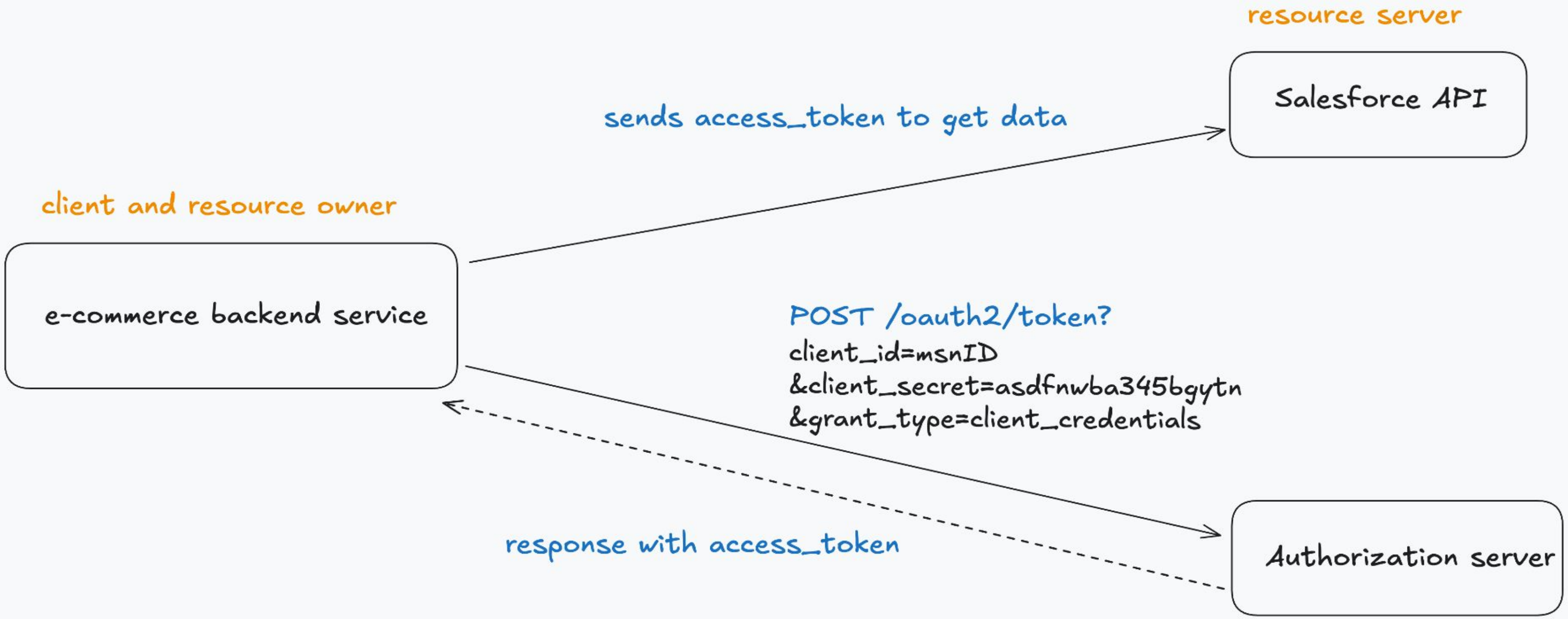
resource server

contacts.google.com

https://datatracker.ietf.org/doc/html/draft-ietf-oauth-browser-based-apps#name-backend-for-frontend-bff

Client credentials flow

- Machine to Machine communication
- client is acting on it's own behalf
- client is also resource owner



resource server

Salesforce API

sends access_token to get data

client and resource owner

e-commerce backend service

POST /oauth2/token?
client_id=msnID
&client_secret=asdfnwba345bgytn
&grant_type=client_credentials

response with access_token

Authorization server

https://auth0.com/docs/get-started/authentication-and-authorization-flow/client-credentials-flow

Code example

https://github.com/GoodbyePlanet/spring-security-friday-talk

Q&A