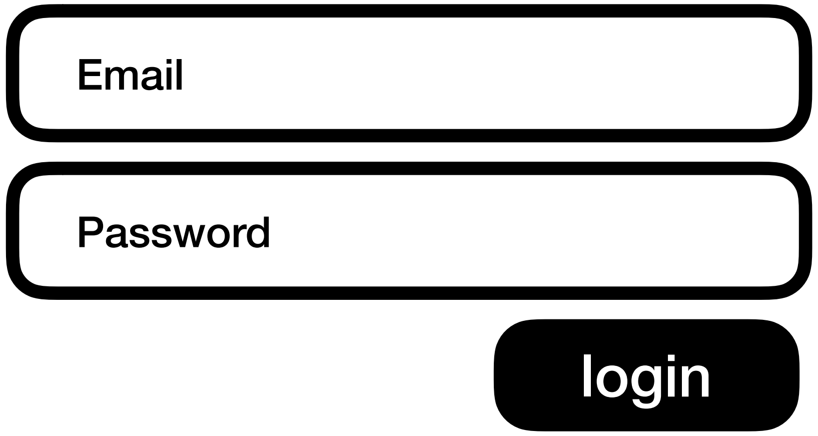
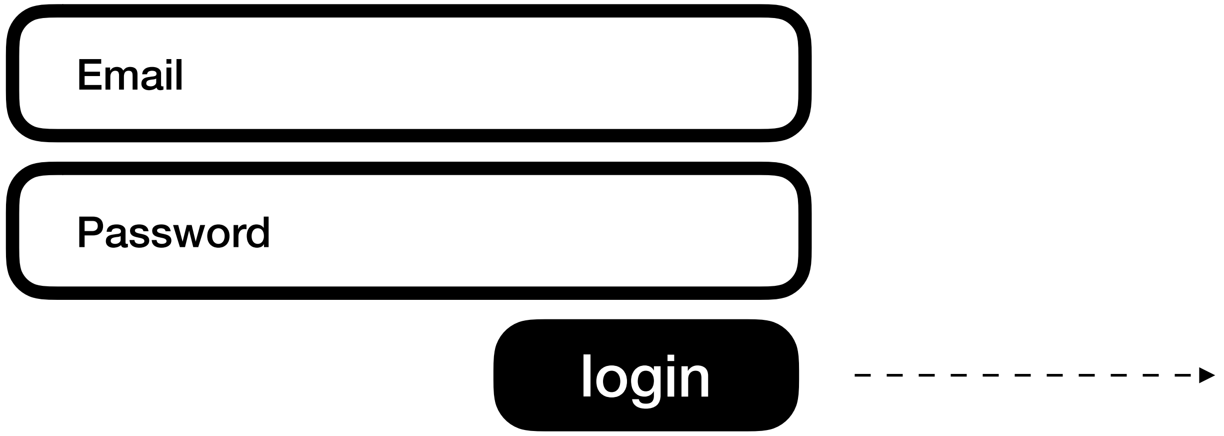
OAuth 2.0 Authorization Code Flow

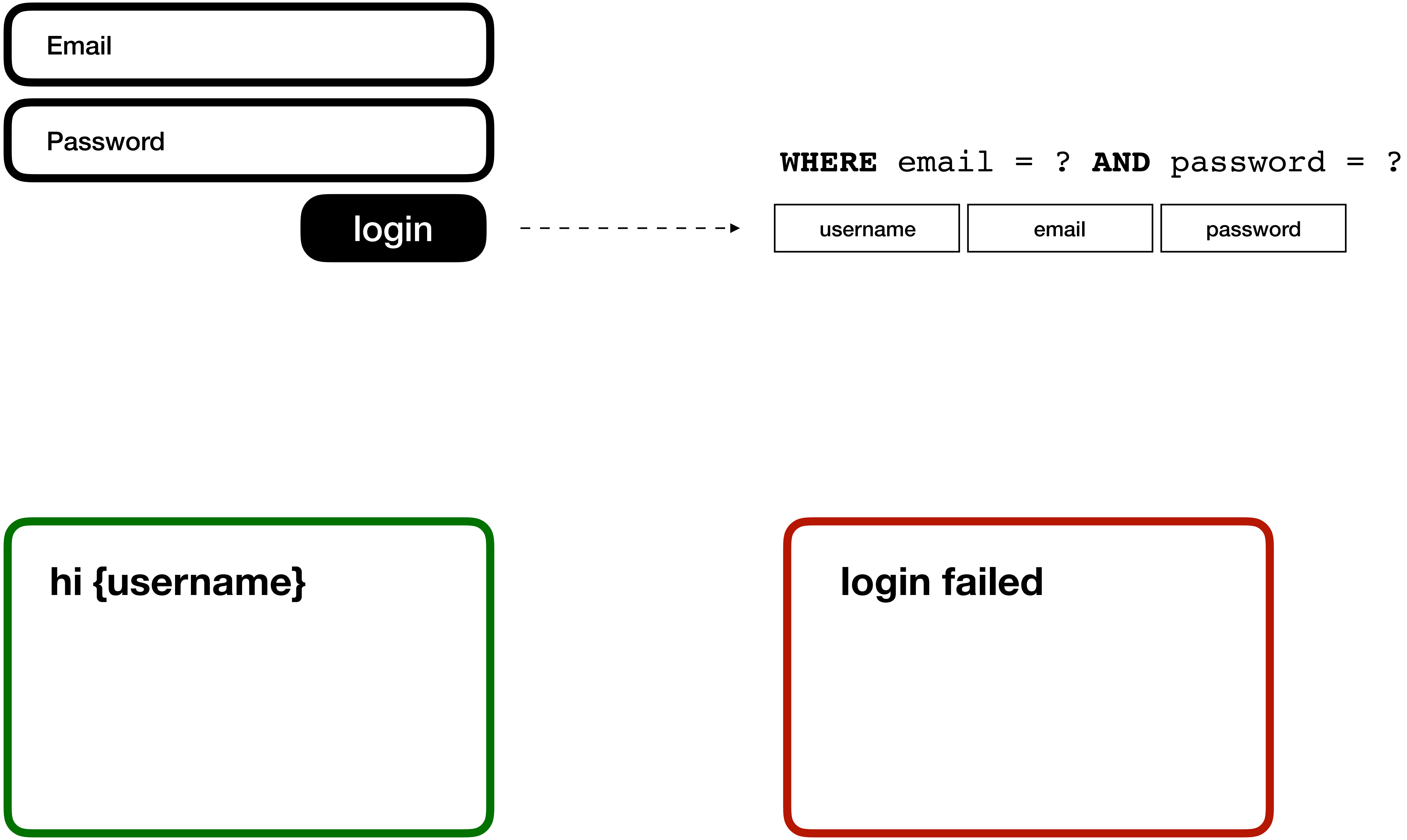
Authentication


Email
Password
login



```
WHERE email = ? AND password = ?
```

username	email	password



Email

Password

login

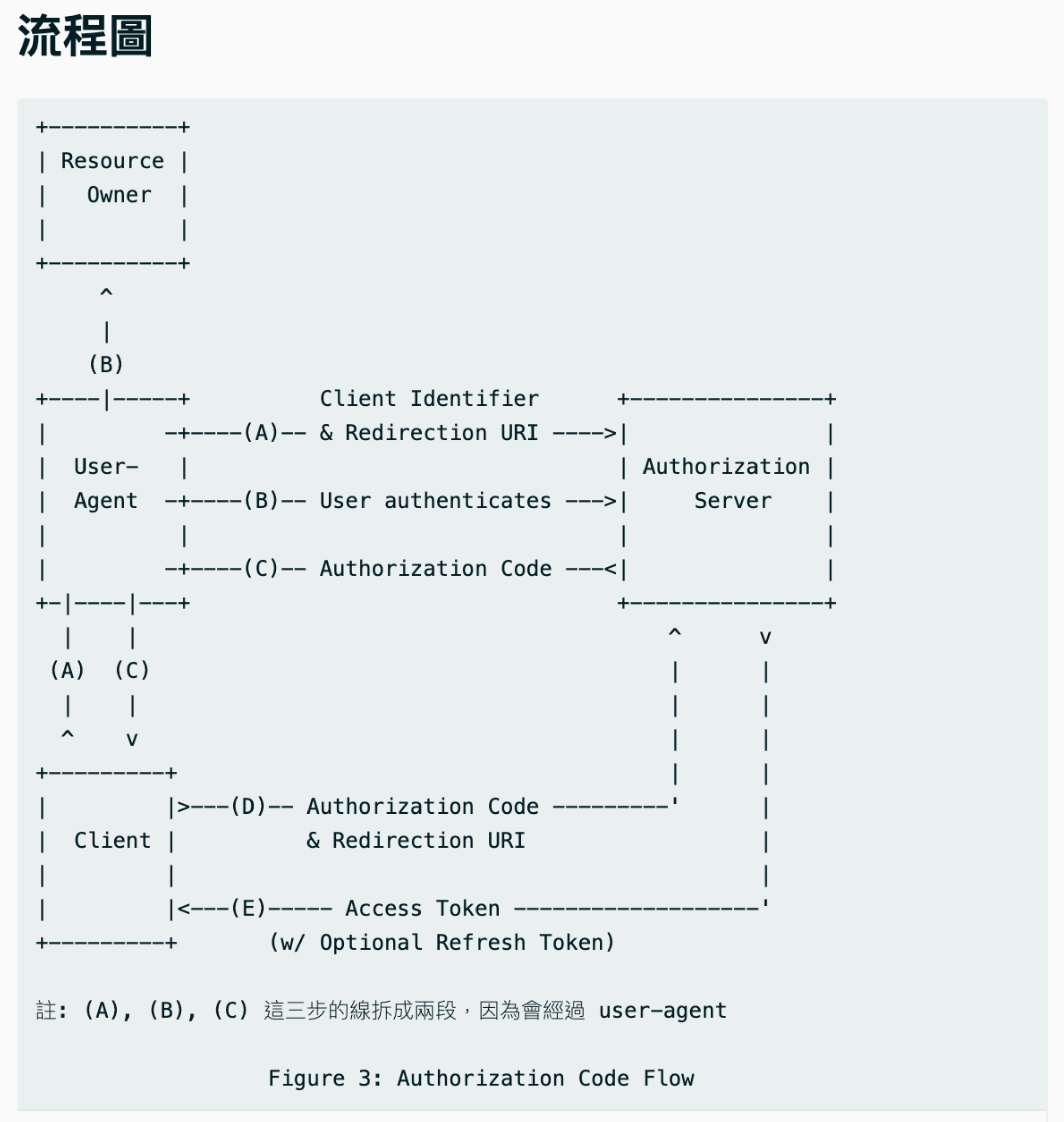
```
WHERE email = ? AND password = ?
```

username	email	password

hi {username}

login failed

Delegated Authorization with OAuth 2.0



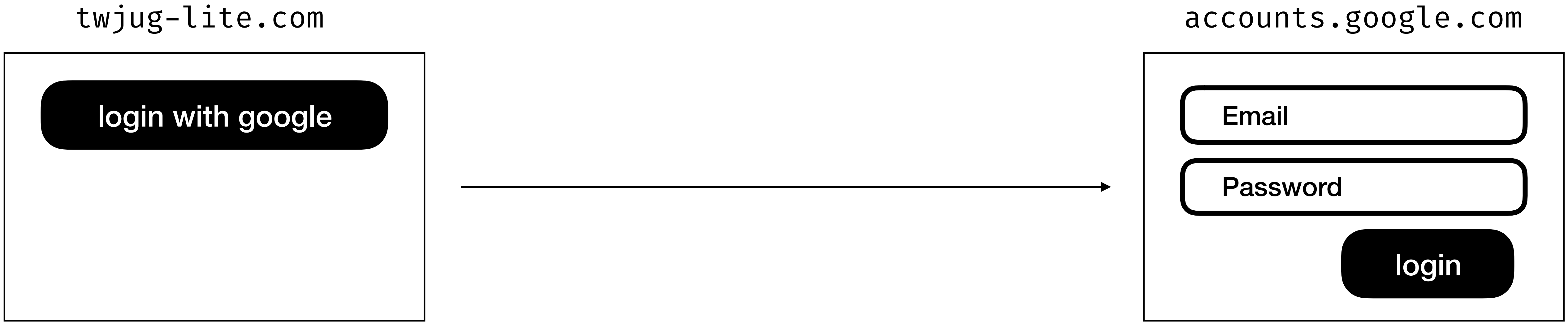
流程圖

```
+----------+
| Resource |
|   Owner  |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier      +---------------+
|         -+----(A)-- & Redirection URI ---->|               |
|  User-   |                                 | Authorization |
|  Agent  -+----(B)-- User authenticates --->|     Server    |
|          |                                 |               |
|         -+----(C)-- Authorization Code ---<|               |
+-|----|---+                                 +---------------+
  |    |                                         ^      v
 (A)  (C)                                        |      |
  |    |                                         |      |
  ^    v                                         |      |
+---------+                                      |      |
|         |>---(D)-- Authorization Code ---------'      |
|  Client |          & Redirection URI                  |
|         |                                             |
|         |<---(E)----- Access Token -------------------'
+---------+       (w/ Optional Refresh Token)
```

註: (A), (B), (C) 這三步的線拆成兩段，因為會經過 user-agent

Figure 3: Authorization Code Flow

https://blog.yorkxin.org/2013/09/30/oauth2-4-1-auth-code-grant-flow.html



twjug-lite.com

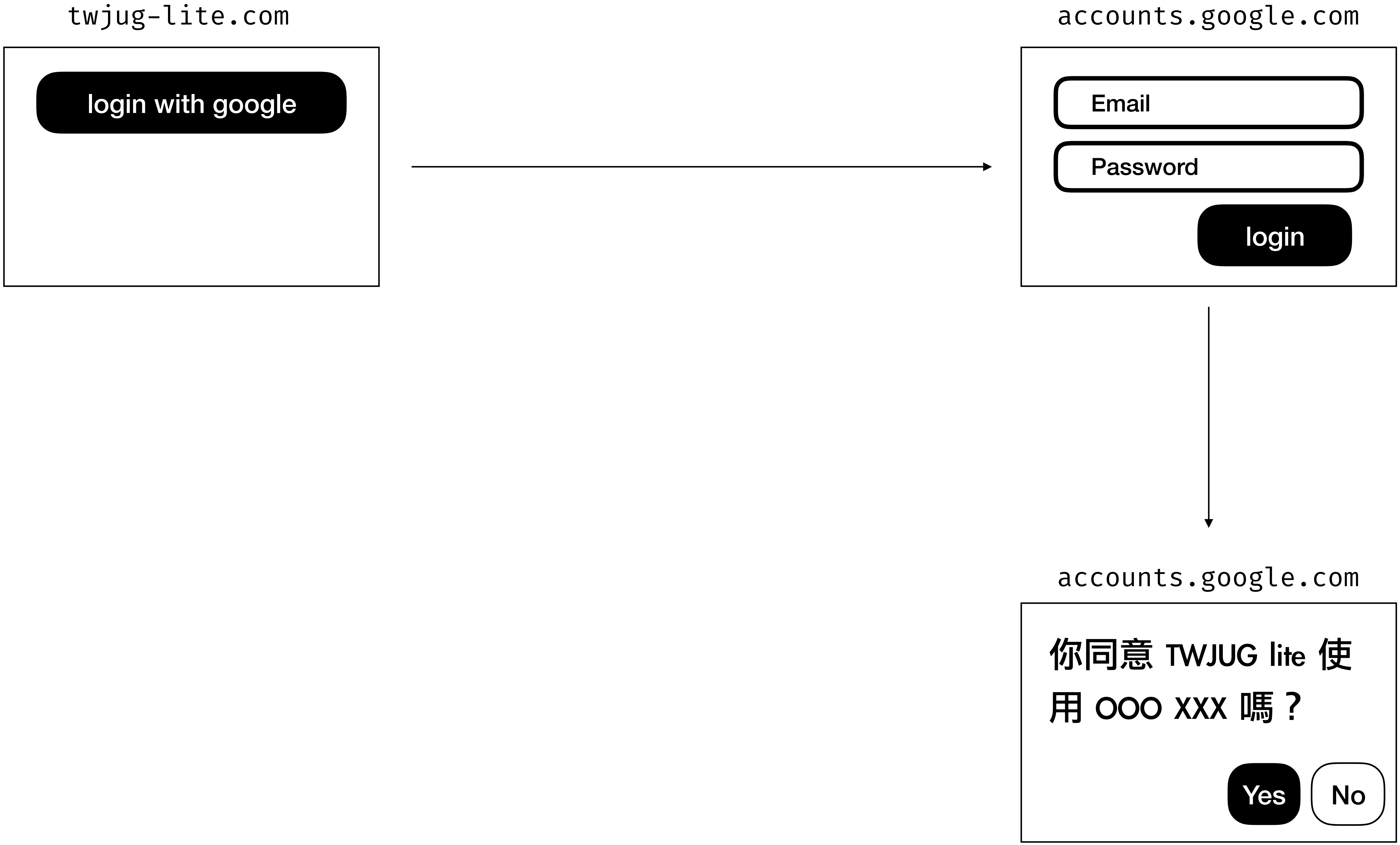
login with google

accounts.google.com

Email

Password

login

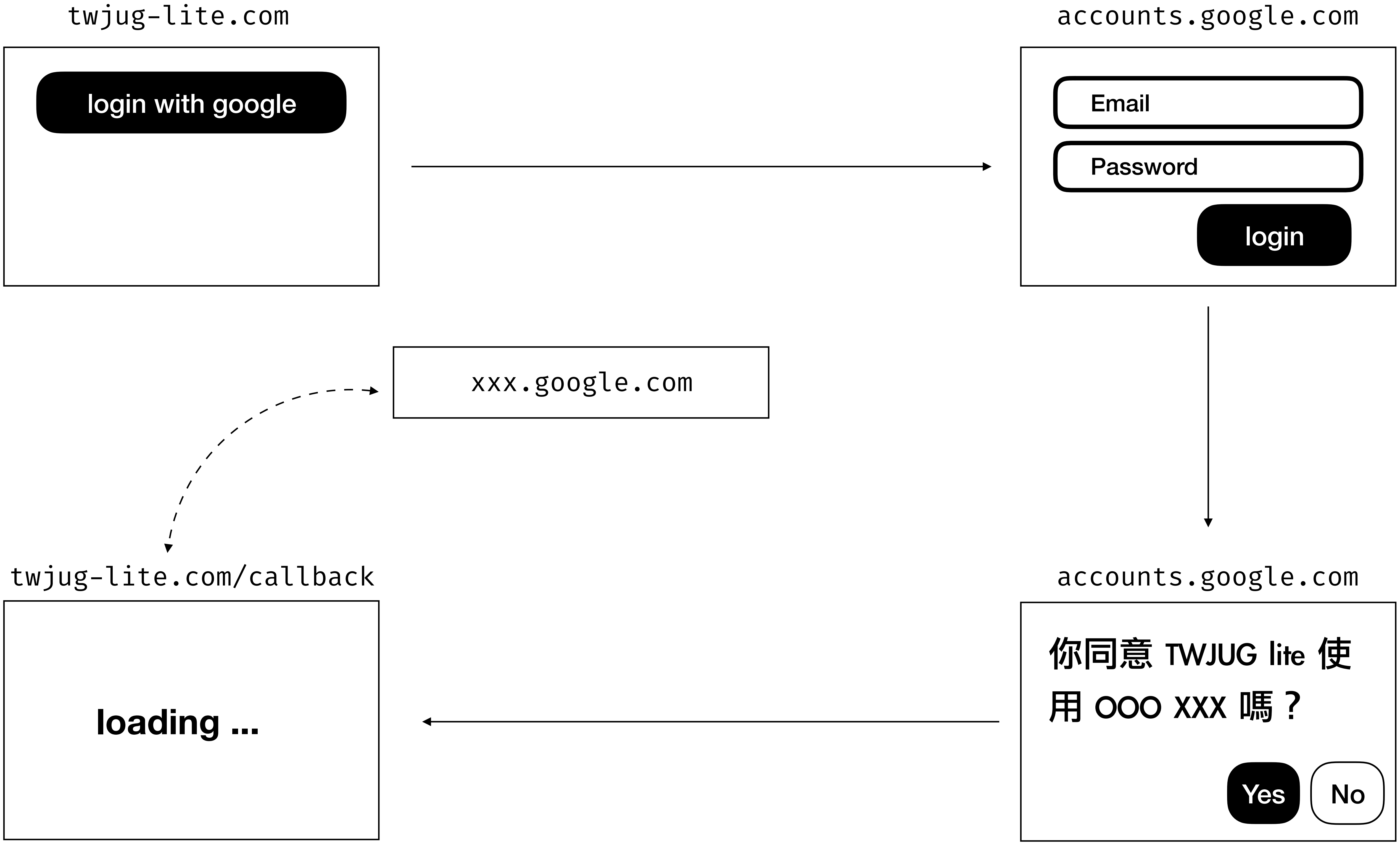


twjug-lite.com

accounts.google.com

accounts.google.com

你同意 TWJUG lite 使用 OOO XXX 嗎？



twjug-lite.com

accounts.google.com

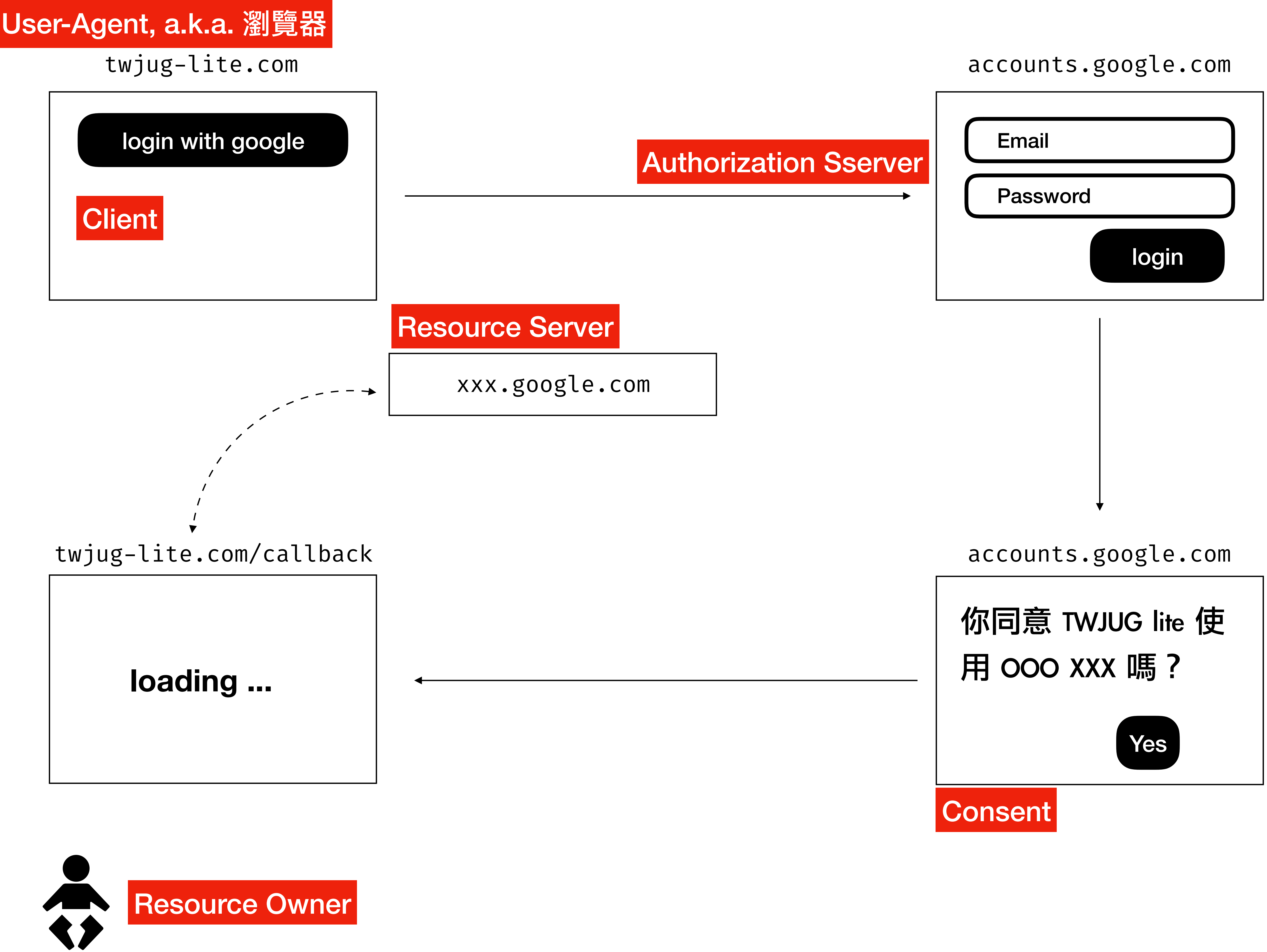
xxx.google.com

twjug-lite.com/callback

loading ...

accounts.google.com

你同意 TWJUG lite 使用 OOO XXX 嗎？



User-Agent, a.k.a. 瀏覽器

twjug-lite.com

login with google

Client

Authorization Sserver

accounts.google.com

Email

Password

login

Resource Server

xxx.google.com

twjug-lite.com/callback

loading ...

accounts.google.com

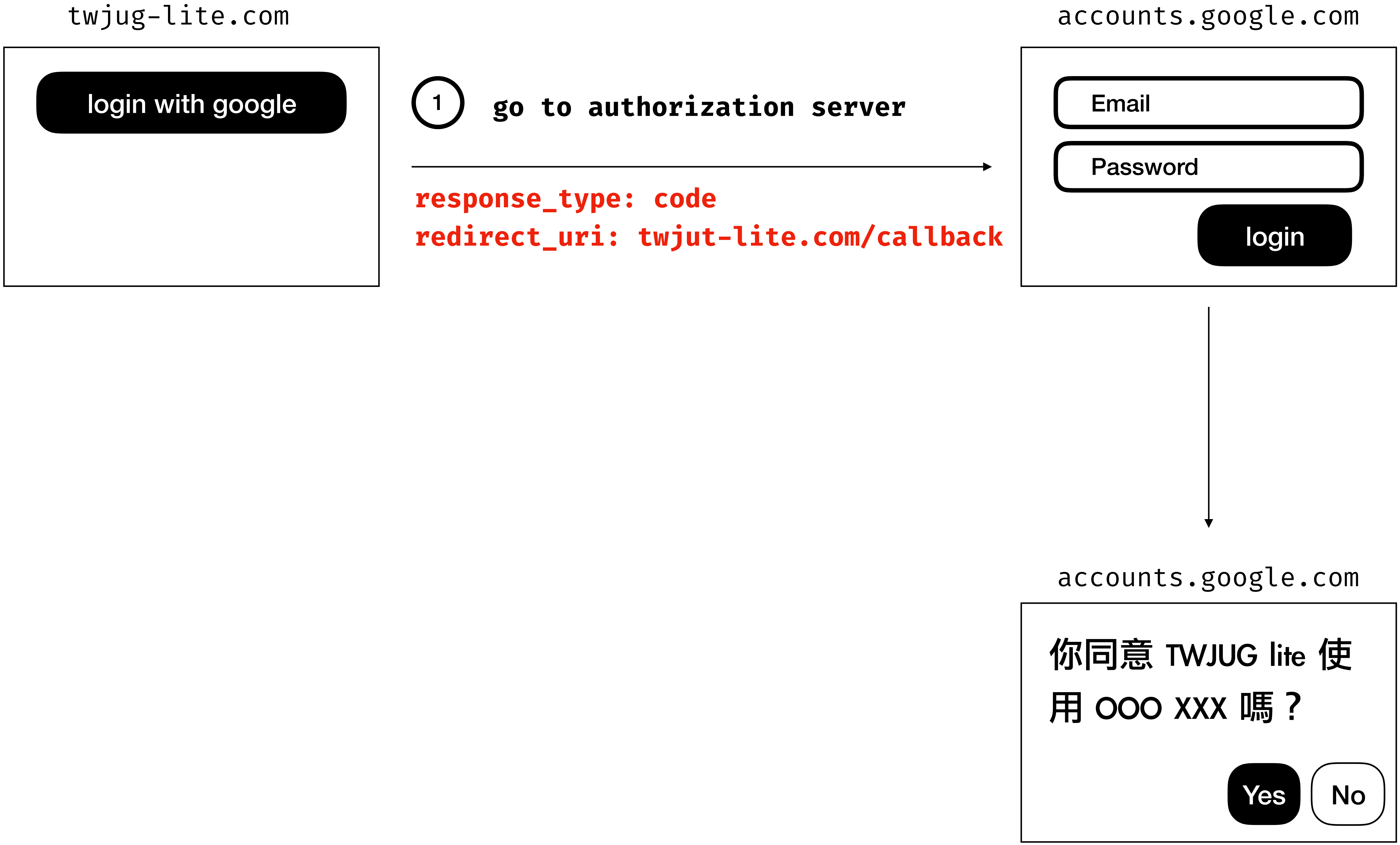
你同意 TWJUG lite 使用 OOO XXX 嗎？

Yes

Consent

Resource Owner

RE: 重零開始的 OAuth Flow 細節生活



twjug-lite.com

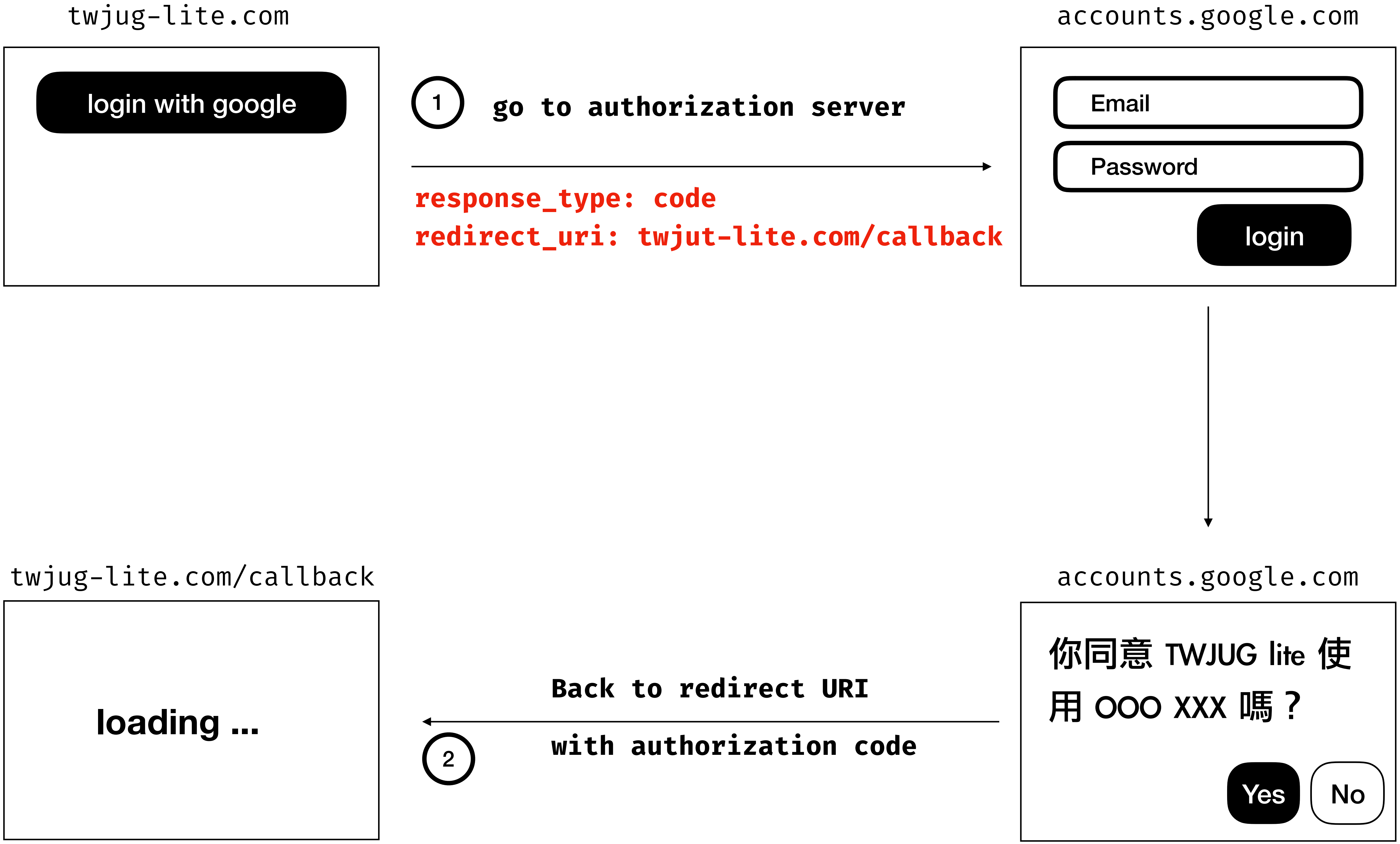
1 go to authorization server

response_type: code
redirect_uri: twjut-lite.com/callback

accounts.google.com

accounts.google.com

你同意 TWJUG lite 使用 OOO XXX 嗎？



twjug-lite.com

login with google

1 go to authorization server

response_type: code
redirect_uri: twjut-lite.com/callback

accounts.google.com

Email

Password

login

accounts.google.com

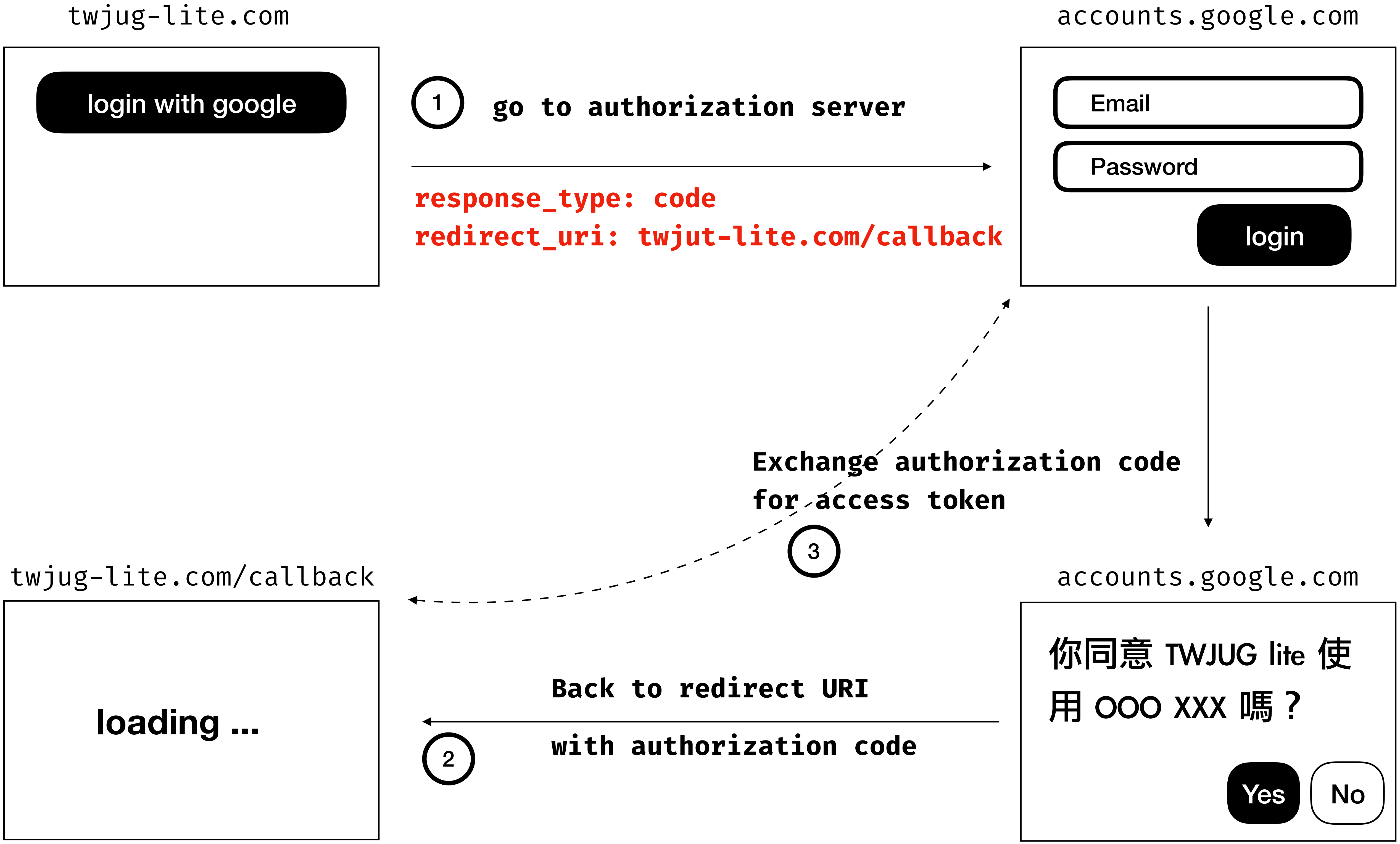
你同意 TWJUG lite 使
用 OOO XXX 嗎？

Yes No

Back to redirect URI
with authorization code
2

twjug-lite.com/callback

loading ...



twjug-lite.com

login with google

1 go to authorization server

response_type: code
redirect_uri: twjut-lite.com/callback

accounts.google.com

Email

Password

login

Exchange authorization code
for access token

3

twjug-lite.com/callback

loading ...

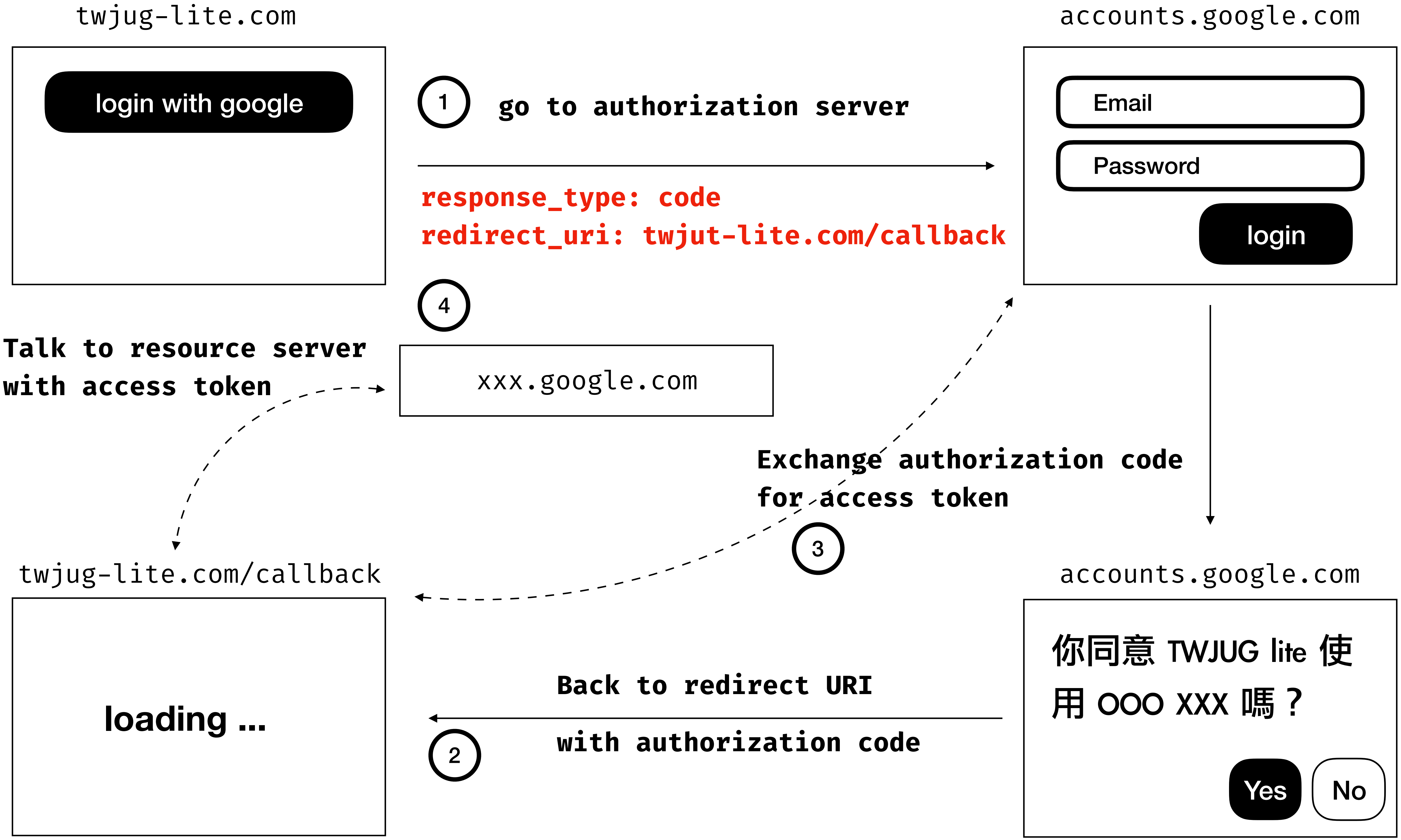
Back to redirect URI

2 with authorization code

accounts.google.com

你同意 TWJUG lite 使
用 OOO XXX 嗎？

Yes No



twjug-lite.com

login with google

1 go to authorization server

response_type: code
redirect_uri: twjut-lite.com/callback

accounts.google.com

Email

Password

login

accounts.google.com

你同意 TWJUG lite 使用 OOO XXX 嗎？

Yes No

2 Back to redirect URI with authorization code

twjug-lite.com/callback

loading ...

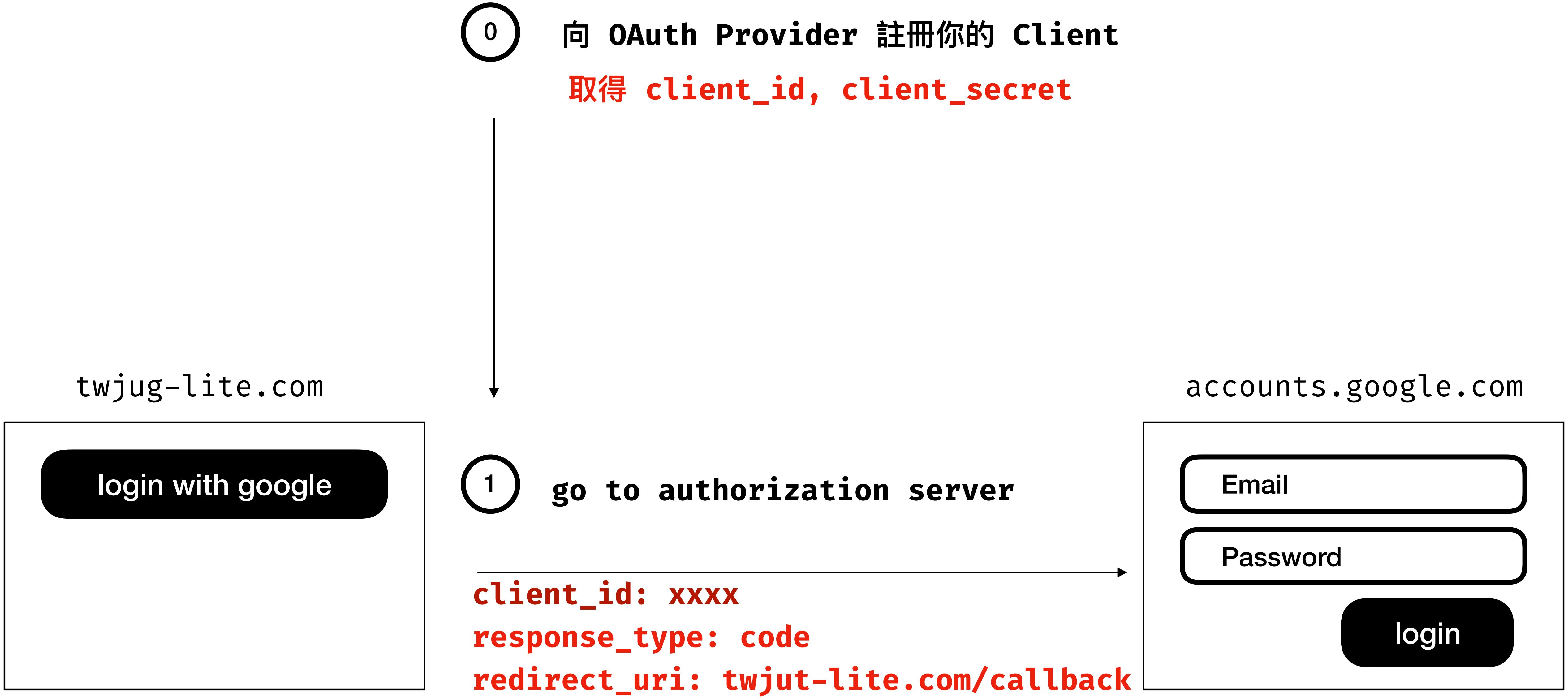
3 Exchange authorization code for access token

4 Talk to resource server with access token

xxx.google.com

動手做看看

https://auth0.com/docs/api-auth/tutorials/authorization-code-grant



0 向 OAuth Provider 註冊你的 Client

取得 client_id, client_secret

twjug-lite.com

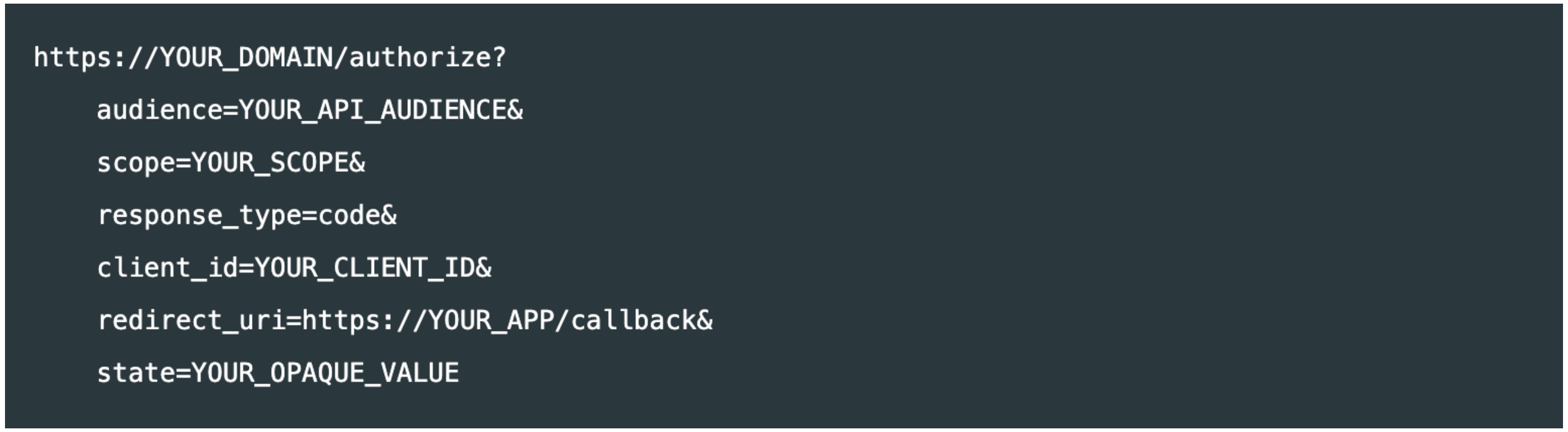
accounts.google.com

1 go to authorization server

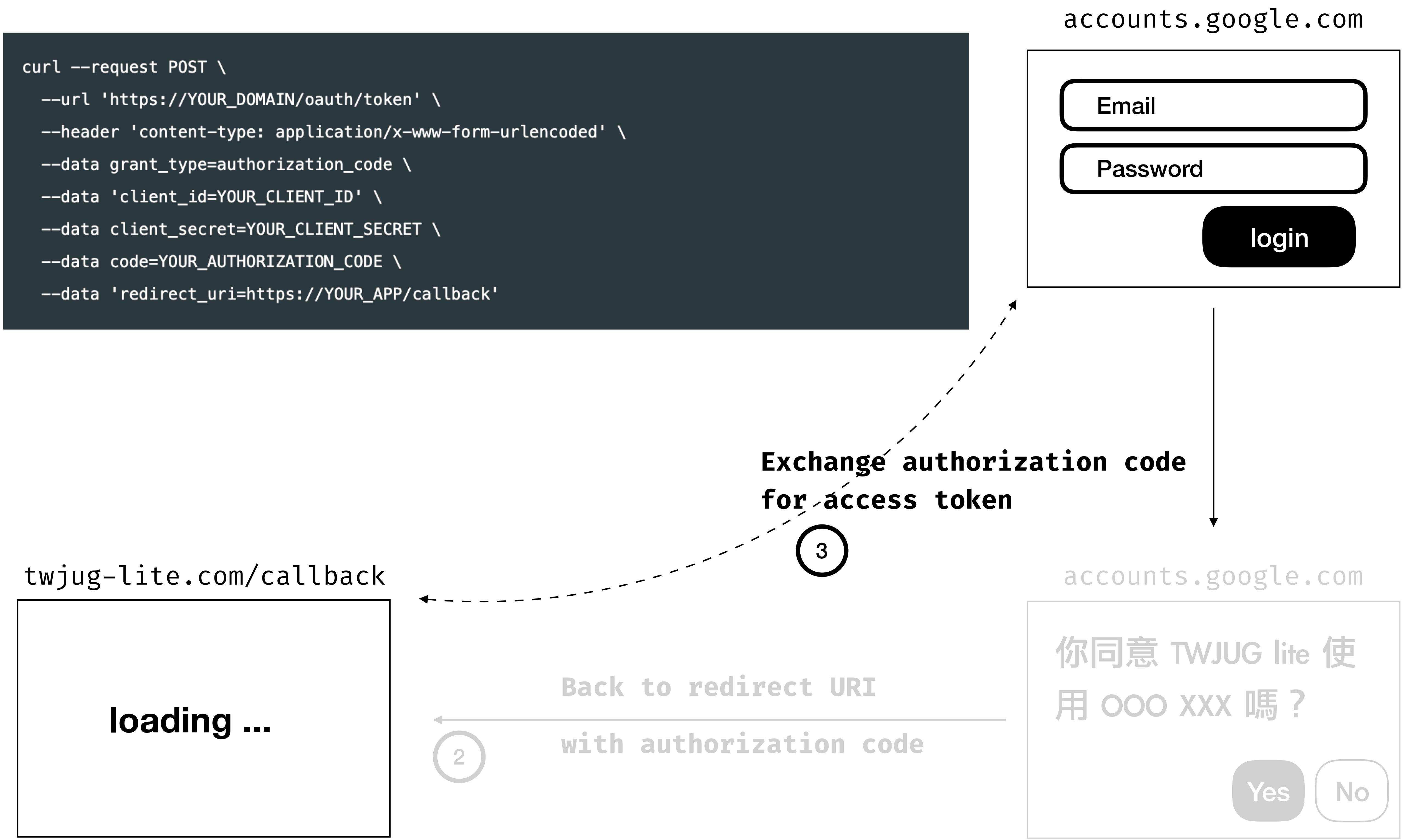
client_id: xxxx

response_type: code

redirect_uri: twjut-lite.com/callback



```
https://YOUR_DOMAIN/authorize?
    audience=YOUR_API_AUDIENCE&
    scope=YOUR_SCOPE&
    response_type=code&
    client_id=YOUR_CLIENT_ID&
    redirect_uri=https://YOUR_APP/callback&
    state=YOUR_OPAQUE_VALUE
```



```
curl --request POST \
  --url 'https://YOUR_DOMAIN/oauth/token' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data grant_type=authorization_code \
  --data 'client_id=YOUR_CLIENT_ID' \
  --data client_secret=YOUR_CLIENT_SECRET \
  --data code=YOUR_AUTHORIZATION_CODE \
  --data 'redirect_uri=https://YOUR_APP/callback'
```