WEB2 - OAuth

순서

1. 등록

    a. Resource Server의 승인을 사전에 받기
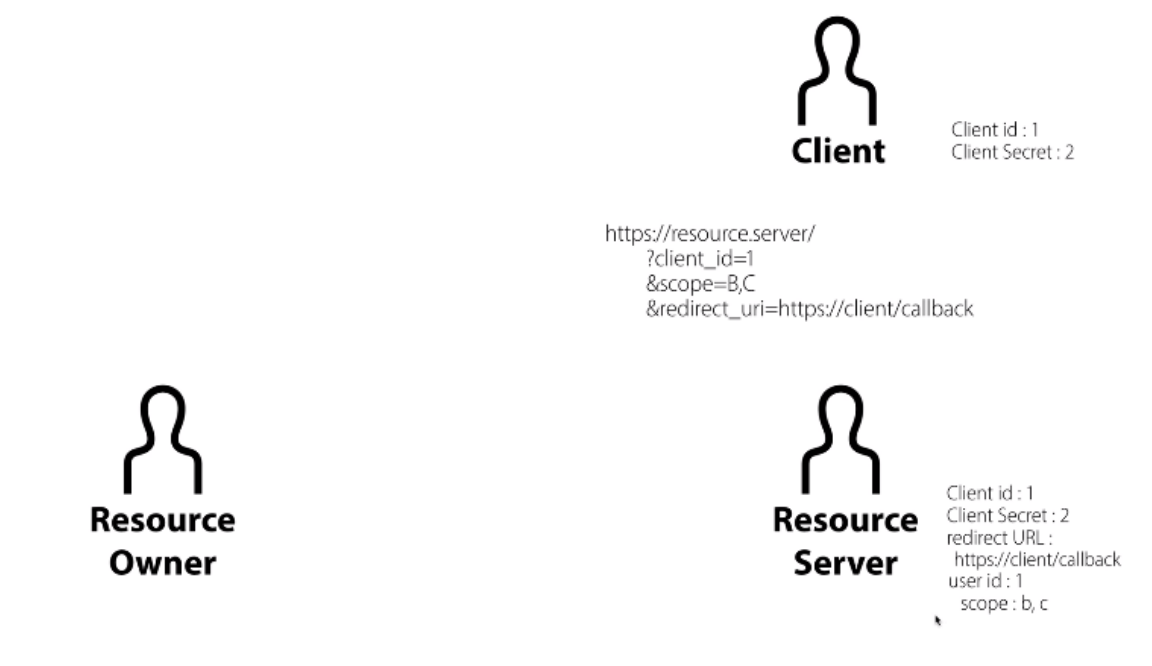

- Secret: 비밀번호 → 외부에 노출 X

- Authorized~: 해당 주소에서 요청

2. Resource Owner 인증
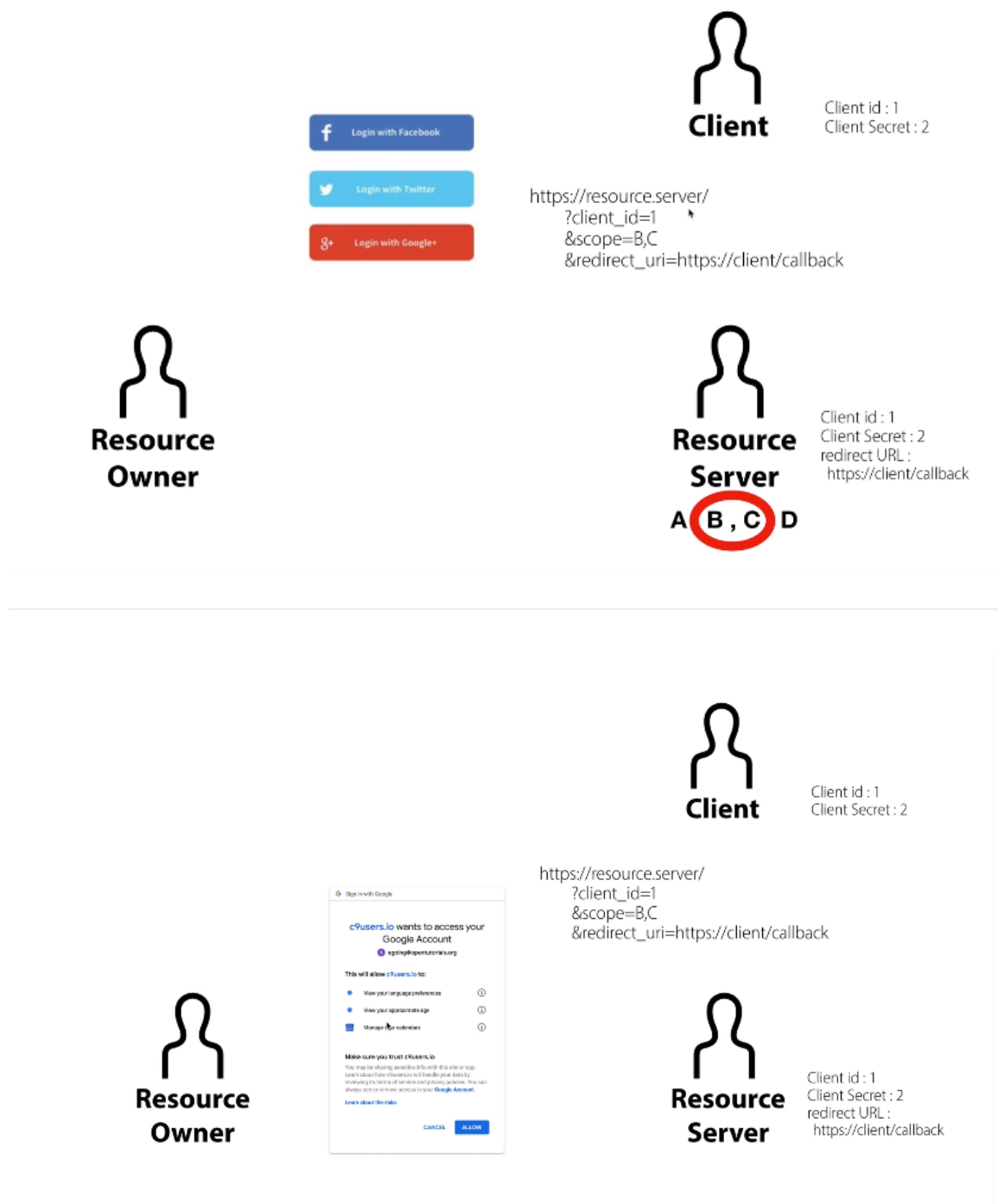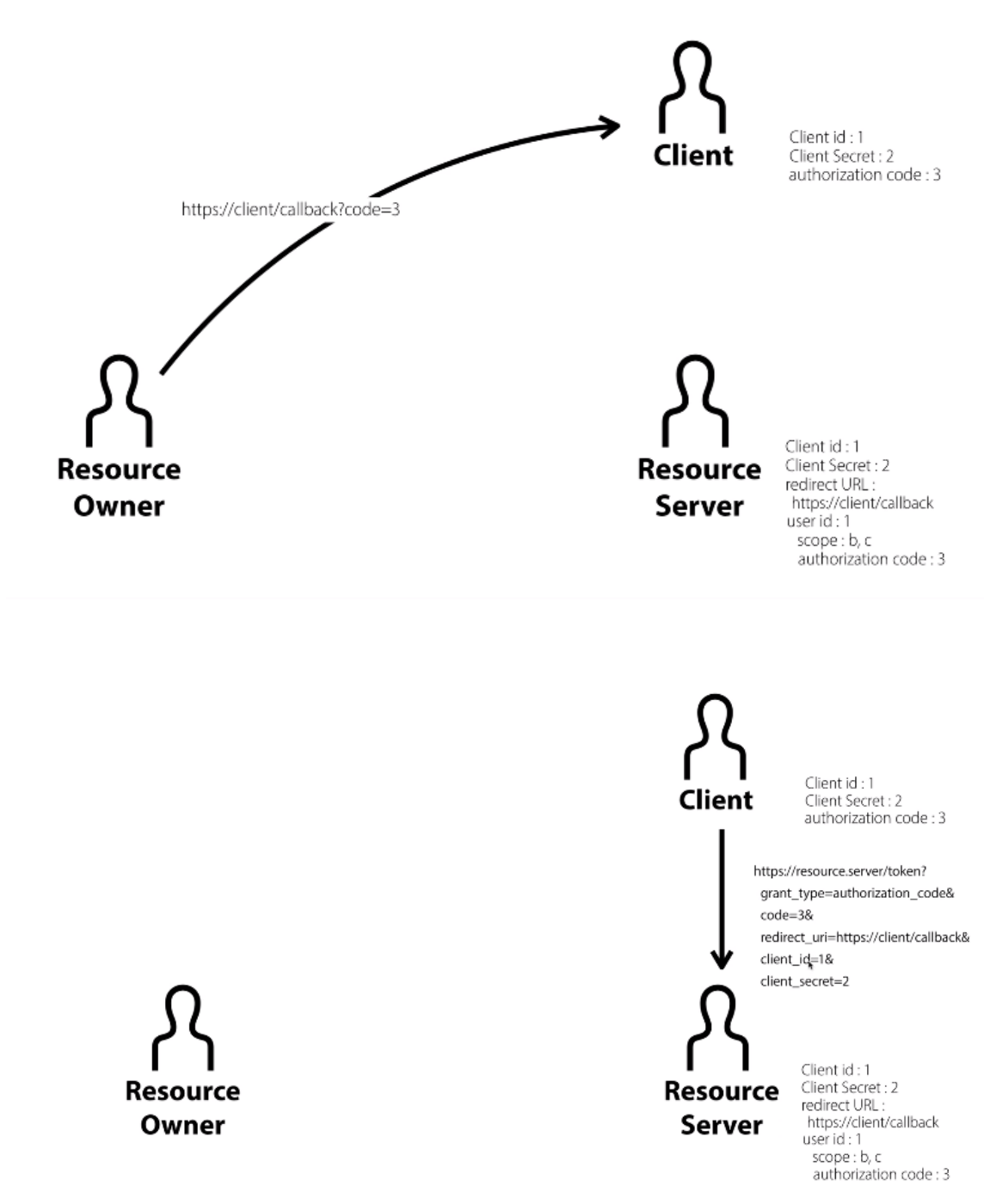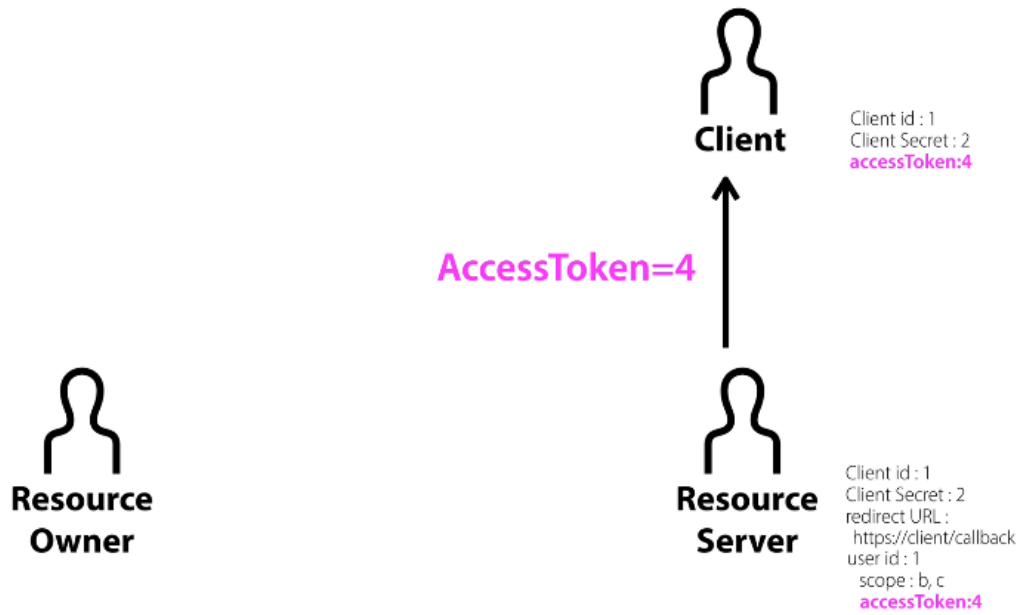
- Resource Owner로부터 정보를 사용해도 좋다는 승인을 Resource Server가 받기

3. Resource Server 승인
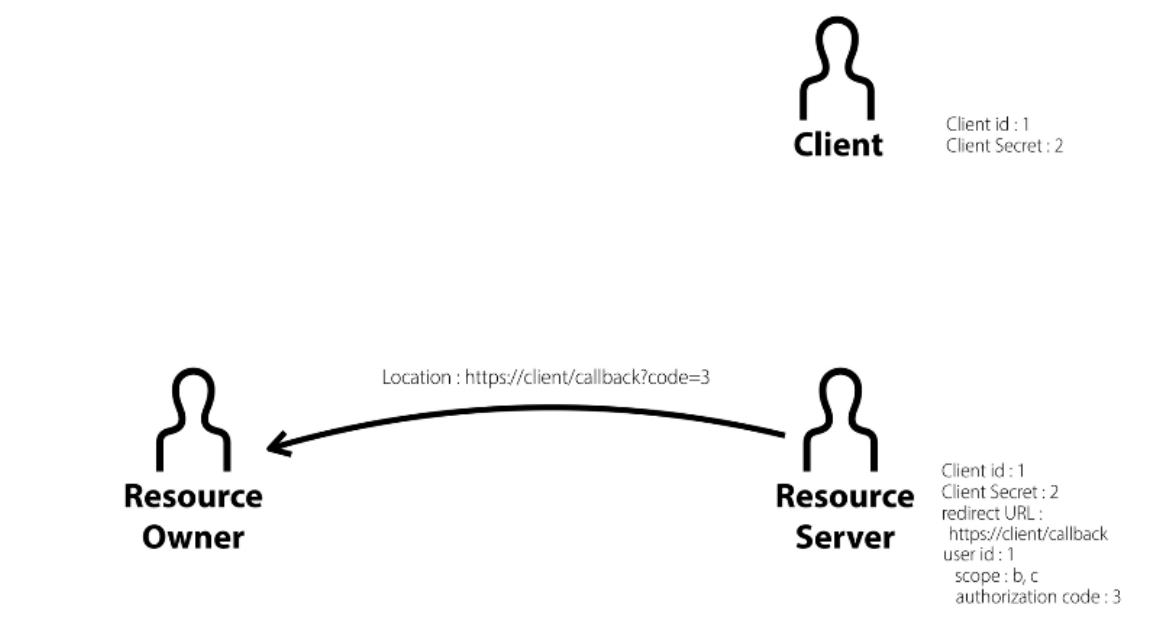
- authorization code와 id, Secret, redirect_url이 일치하는지 확인

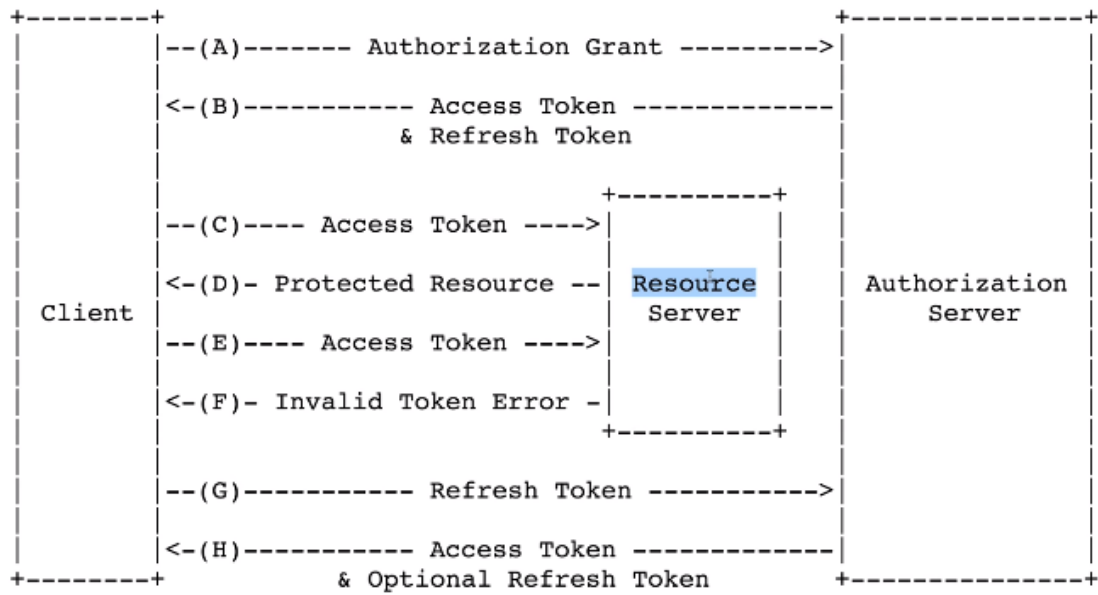4. 액세스 토큰 발급

Client id : 1
Client Secret : 2
accessToken:4

AccessToken=4

Client id : 1
Client Secret : 2
redirect URL :
 https://client/callback
user id : 1
 scope : b, c
accessToken:4

5. API 호출
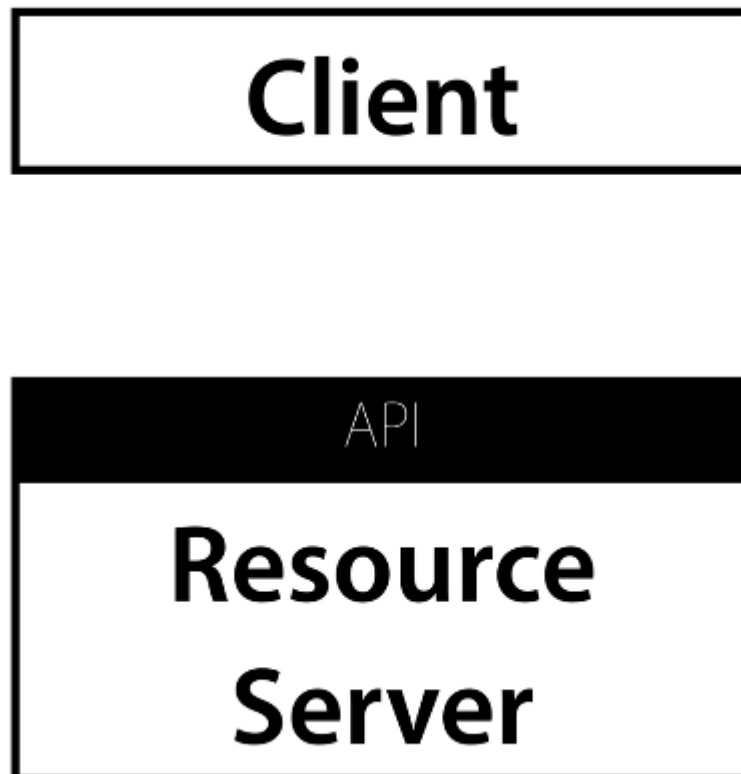
- OAuth를 통해 access token 가져오기

6. refresh token

- access token: 수명이 있음
  - 다시 발급 필요

```
+--------+                                        +--------------+
|        |--(A)------- Authorization Grant -------->|              |
|        |                                        |              |
|        |<-(B)----------- Access Token -----------|              |
|        |              & Refresh Token            |              |
|        |                                        |              |
|        |                      +----------+      |              |
|        |--(C)---- Access Token ---->|          |      |              |
|        |                      |          |      |              |
|        |<-(D)- Protected Resource --| Resource |      | Authorization|
| Client |                      | Server   |      |    Server    |
|        |--(E)---- Access Token ---->|          |      |              |
|        |                      |          |      |              |
|        |<-(F)- Invalid Token Error -|          |      |              |
|        |                      +----------+      |              |
|        |                                        |              |
|        |--(G)----------- Refresh Token ---------->|              |
|        |                                        |              |
|        |<-(H)----------- Access Token -----------|              |
+--------+         & Optional Refresh Token         +--------------+
```

- federated identity
- Restful, JSON, XML → API