Daum OAuth 2.0

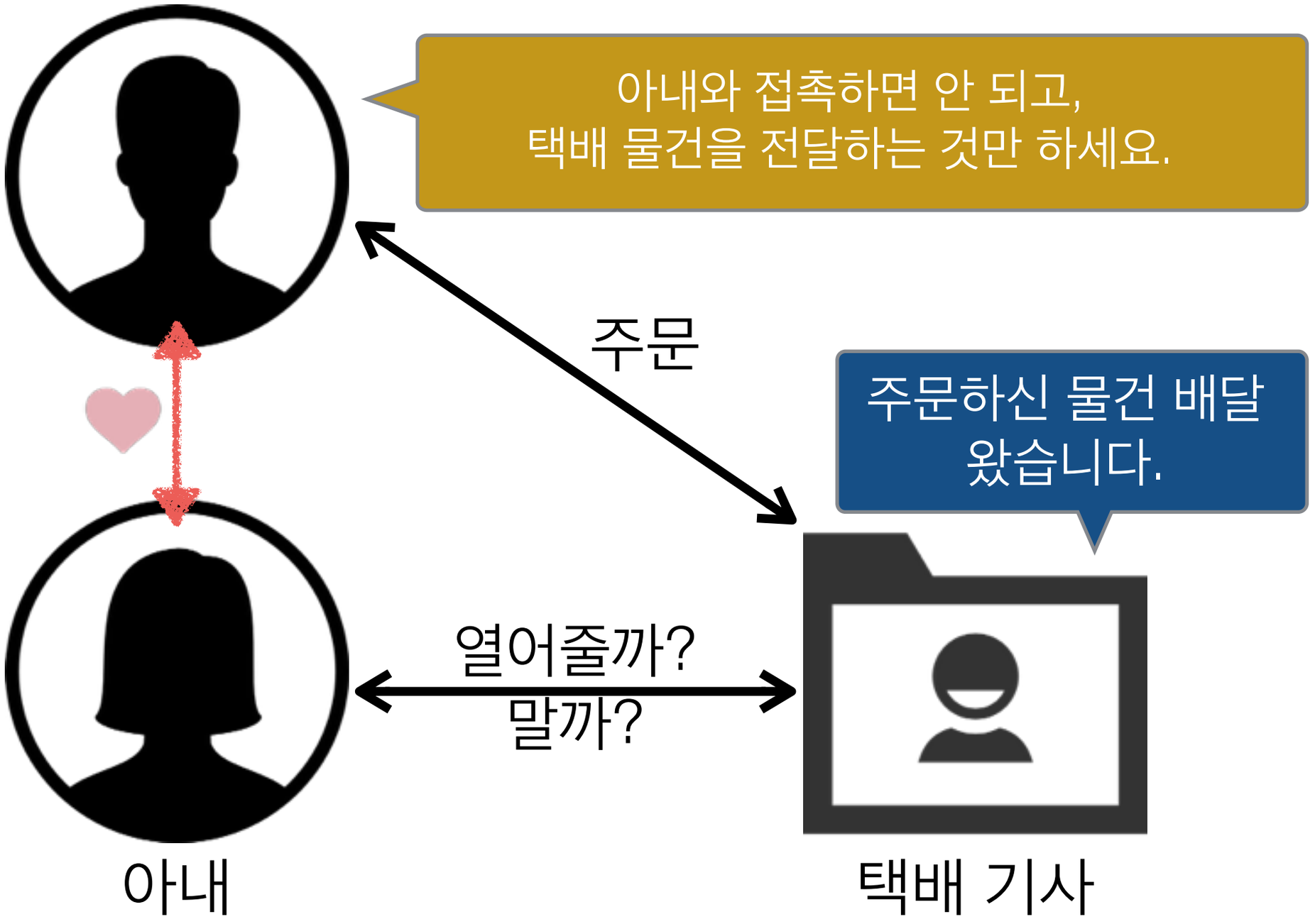
Daum 클라우드기술팀
이승철

2014 Daum API 부트캠프

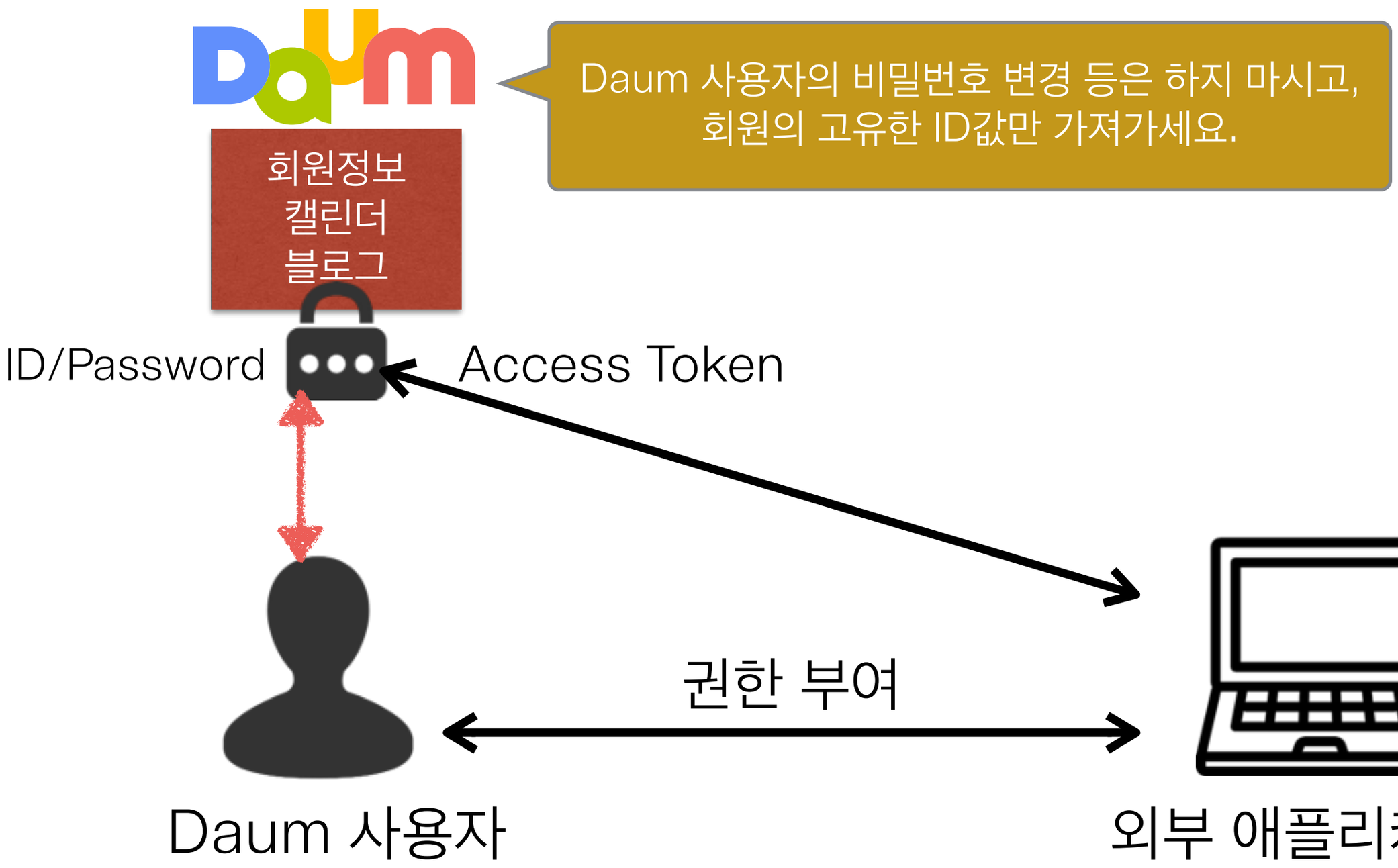
소개

- 이승철 (tadoli)
- Daum 클라우드기술팀
- 사내외 API 플랫폼 개발/운영

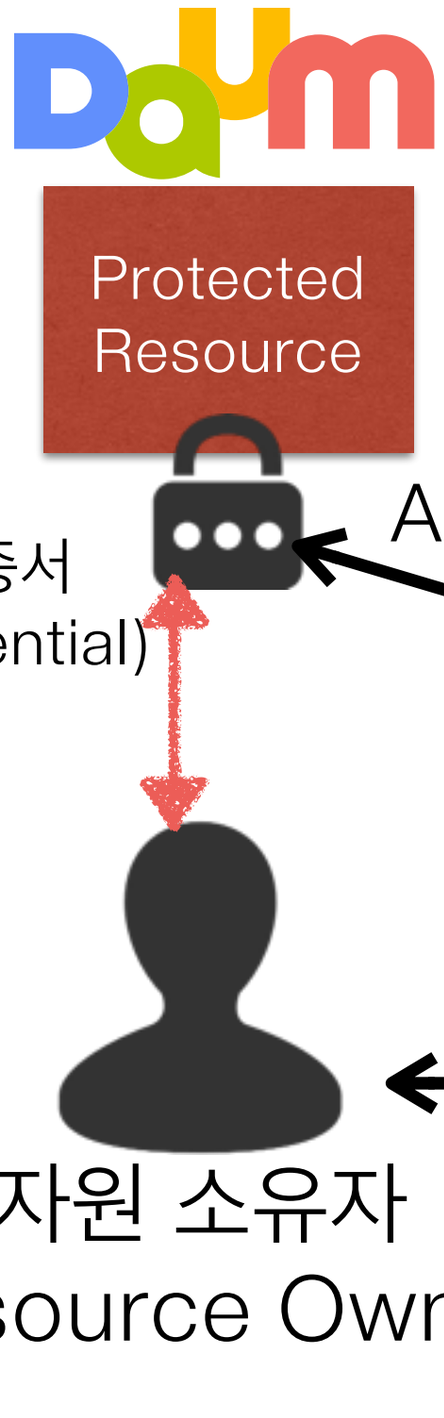
사랑의 삼각 관계


아내와 접촉하면 안 되고,
택배 물건을 전달하는 것만 하세요.
주문
주문하신 물건 배달
왔습니다.
열어줄까?
말까?
아내
택배 기사

OAuth의 삼각 관계


Daum
회원정보
캘린더
블로그
Daum 사용자의 비밀번호 변경 등은 하지 마시고,
회원의 고유한 ID값만 가져가세요.
ID/Password
Access Token
권한 부여
Daum 사용자
외부 애플리케이션

OAuth 2.0 표현



권한 서버(Authorization Server)

자원 서버(Resource Server)

OAuth 2.0

- RFC 6749
- 외부 애플리케이션에서 HTTP 서비스에 제한된 접근을 할 수 있도록 권한을 부여(Authorize)하는 프레임워크

OAuth의 4가지 역할

자원 서버

권한 서버

자원 소유자

클라이언트

OAuth 1.0 vs 2.0 용어

용어	1.0	2.0
사용자	User	Resource Owner
클라이언트	Consumer	Client
API 서버	Service Provider	Resource Server
권한 서버		Authorization Server

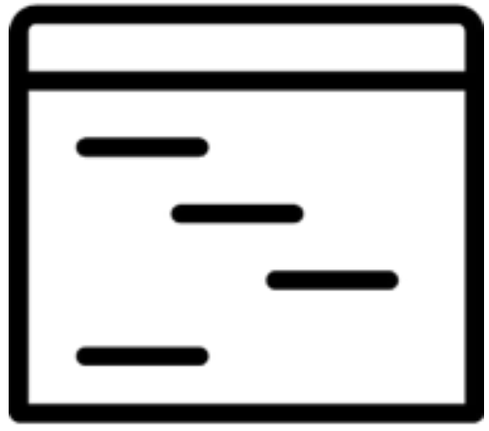
OAuth 1.0 vs 2.0 특징

구분	1.0	2.0
HTTPS	선택	필수
구현 복잡도	복잡 (signature 생성)	비교적 간단
보안상 안전한 환경	Server-Side	다양한 환경 지원

클라이언트 유형

기밀 클라이언트
(Confidential Client)

소스코드의 공개 여부



공개 클라이언트
(Public Client)

클라이언트 예

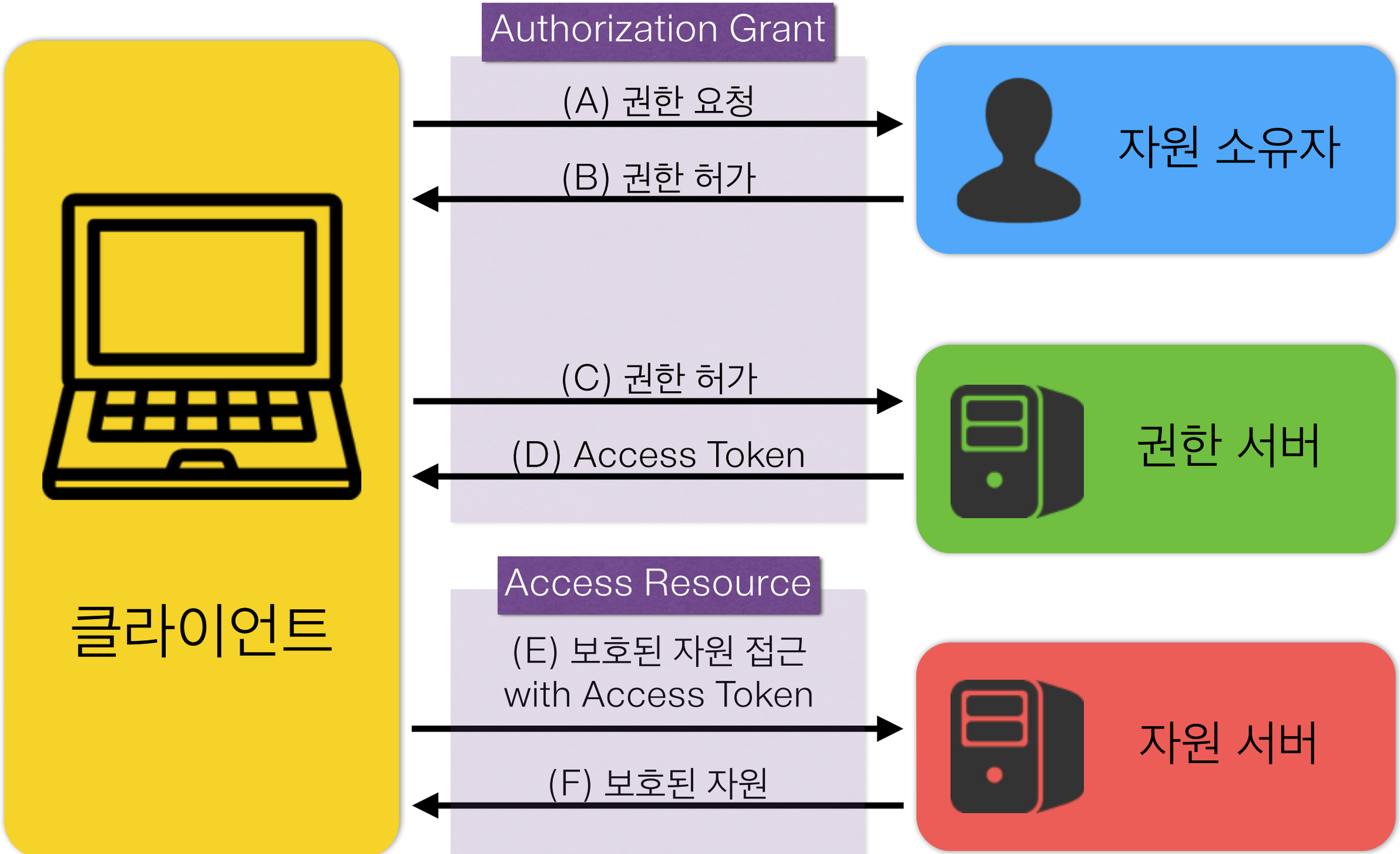
- Server-side 애플리케이션 (on 웹 서버)
  - 기밀 클라이언트
- 사용자 에이전트 애플리케이션 (on 웹브라우저)
  - 공개 클라이언트
- 네이티브 애플리케이션
  - 공개 클라이언트

OAuth 1.0 vs 2.0

기본적인 개념만 비슷할 뿐…

전혀 호환되지 않음!

OAuth 2.0 Protocol



Demo

http://tadoli.net/login/oauth2/exam/daum_exam.html

Authorization Grant

A. 클라이언트가 자원 소유자에게 권한을 달라고 요청
B. 자원 소유자가 클라이언트에 권한 위임 허가
C. 클라이언트는 권한 서버에게 자원 소유자가 허가했다고 알림
D. 권한 서버는 정말 사용자가 허가한게 맞는지 확인 후 Access Token을 클라이언트에 발급

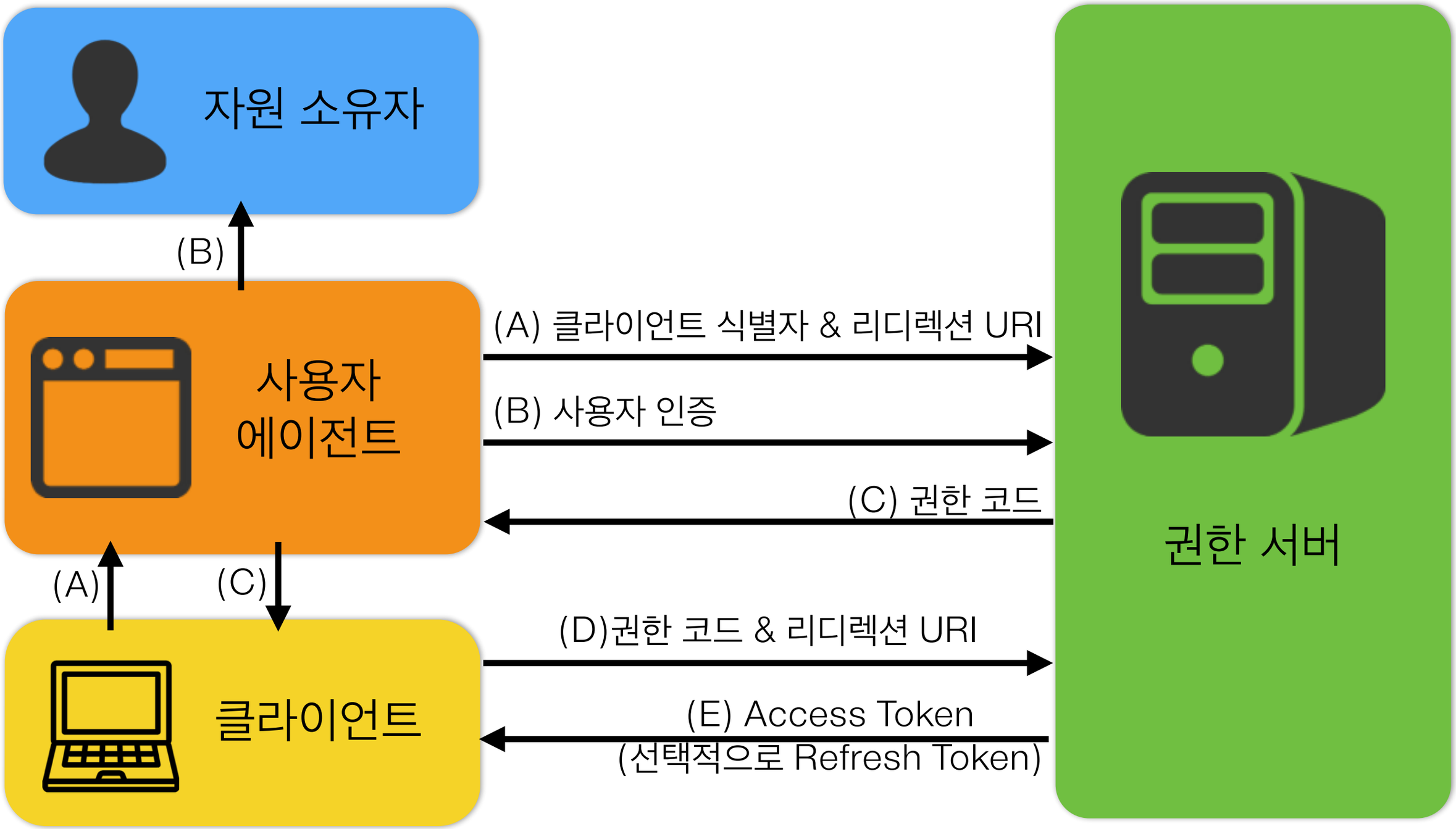
Authorization Grant Type

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant

Authorization Code Grant

- 권한 코드를 이용한 허가 방식
- 장기 접근시 사용
  - Access Token 만료시, Refresh Token 으로 갱신
- 기밀 클라이언트일 때 사용

Authorization Code Grant



End Point

- https://apis.daum.net/oauth2/authorize
- https://apis.daum.net/oauth2/token

Authorization 요청

- Authorization Code Grant -

- response_type: “code” 여야 함.
- client_id: 클라이언트 식별자.
- redirect_uri: 응답시, redirect될 URI.
- scope : 접근 요청 범위

Authorization 응답

- Authorization Code Grant -

- code: 필수. 권한 서버가 생성한 권한 코드

Access Token 요청

- Authorization Code Grant -

- grant_type: “authorization_code” 여야 함.
- code : 권한 서버로부터 받은 코드값
- client_id : 클라이언트 식별자
- client_secret : 클라이언트 시크릿
- redirect_uri : redirect 될 URI

Access Token 응답

- Authorization Code Grant -

- access_token: 필수. 권한 서버가 생성한 권한 코드
- expires_in : 만료 시간(초 단위)
- refresh_token : 갱신 토큰

Access Token

- ID, Password를 대신하여 자원에 접근하기 위한 값
- 제한된 접근 권한만 갖는다.
- 만료 시간이 존재한다.

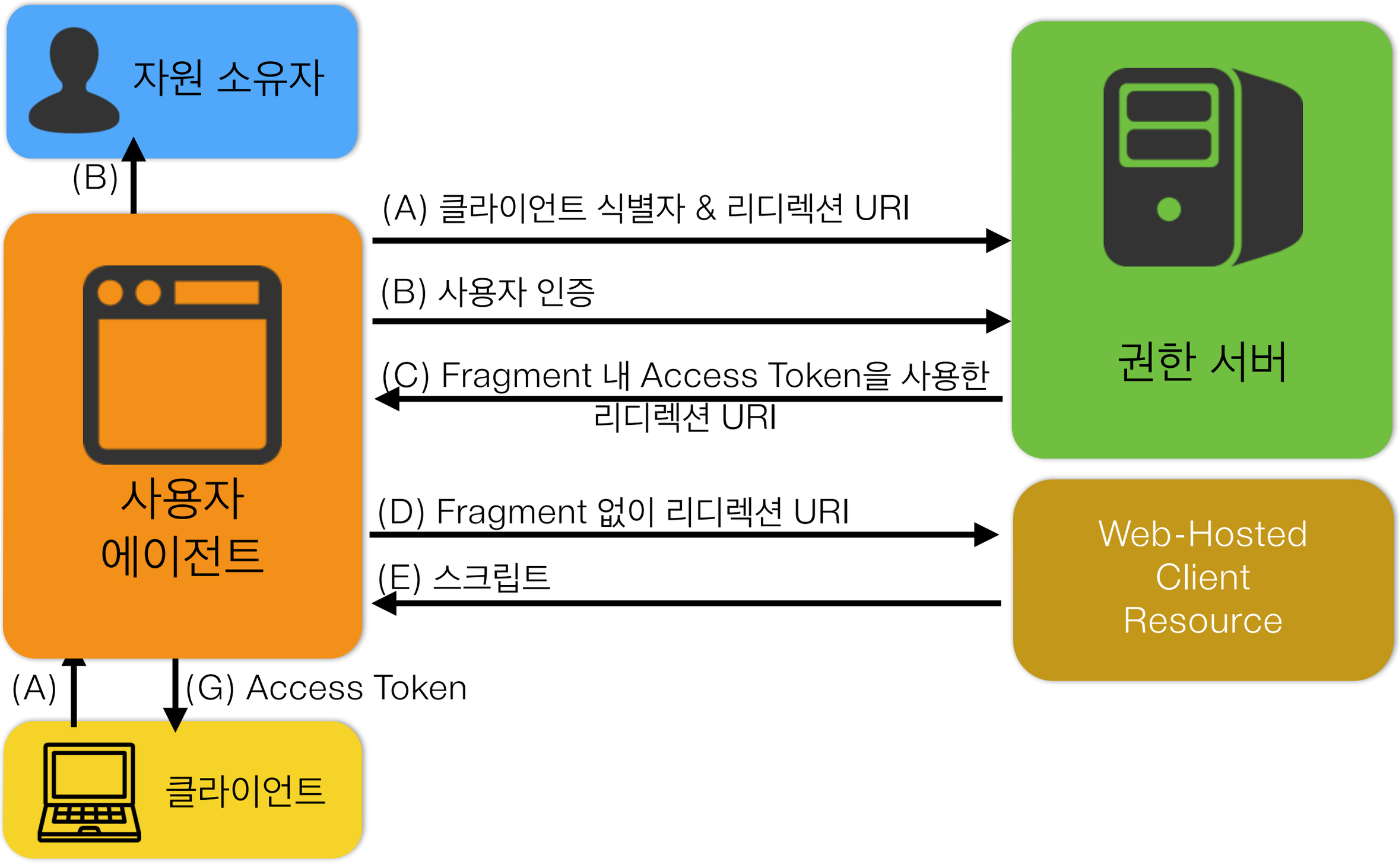
Refresh Token

- Access Token을 얻는데 사용되는 인증서(credential)
- Access Token이 발행될 때 함께 얻을 수 있음
- Access Token이 무효화(invalid)되거나 만료(expire)될 때 사용
- 클라이언트와 권한 서버에서만 알아야 되는 값. 유출되면 보안상 위험.
- 권한서버에서의 지원은 선택적 (Daum에서는 지원함)

Implicit Grant

- 암묵적 허가 방식 - authorize 단계 후, 바로 토큰 발급
- 일시적 접근시 사용
    - Access Token 만료시, 다시 Authorize
- 공개 클라이언트일 때 사용

Implicit Grant



권한 요청

- Implicit Grant -

- response_type: “token” 이어야 함.
- client_id: 클라이언트 식별자
- redirect_uri: redirect될 URI
- scope : 접근 요청의 범위

엑세스 토큰 응답

- Implicit Grant -

- access_token: 권한 서버가 발행한 엑세스 토큰
- token_type: 토큰의 유형 (항상 “Bearer”)
- expires_in: 엑세스 토큰의 수명. 초 단위
- scope: 접근 요청의 범위

Access Resource

Access Resource

- access_token을 실어서 자원 서버로 API를 호출
- Bearer Token ⟵ RFC6750
  - Authorization Request Header Field
  - Form-Encoded Body Parameter
  - URI Query Parameter

Authorization Request Header Field

GET /resource/1 HTTP/1.1
Host: example.com
Authorization: Bearer mF_9.B5f-4.1JqM

Access Token

URI Query Parameter

GET /resource?access_token=mF_9.B5f-4.1JqM HTTP/1.1
Host: example.com

Access Token

OAuth 2.0 사용하려면..

클라이언트
개발자

제휴 신청

Client ID, Secret 발급

무분별한 Client 생성 방지 차원에서 검토 후 발급

별도의 금전적 제휴 비용을 받지는 않음

Daum OAuth 1.0

2014년 말 서비스 중지 예정

구현은 실습 시간에…

감사합니다.