



소셜 로그인

소셜 로그인



소셜 로그인 개념

‘어떻게 구글이나 페이스북으로 가입한 적이 없는 서비스에 로그인을 할 수 있지?’

OAuth2

인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 애플리케이션의 접근 권한을 부여할 수 있는 개방형 표준

사용자가 애플리케이션에게 모든 권한을 넘기지 않고 사용자 대신 서비스를 이용할 수 있게 해주는 HTTP 기반의 보안 프로토콜

사용자 입장 : 여러 서비스들을 하나의 계정으로 관리할 수 있게 되어 편함

개발자 입장 : 민감한 사용자 정보를 다루지 않아 위험 부담이 줄고 서비스 제공자로부터 사용자 정보를 활용 할 수 있음

연동 을 하기 위해 필수로 서비스에 가입된 상태여야 한다.

서비스 제공자로 부터 사용자 인증 및 허가를 받는다.

인증자의 정보를 받아 가입한 계정에 저장을 하면 **연동** 이 되는 것이다.

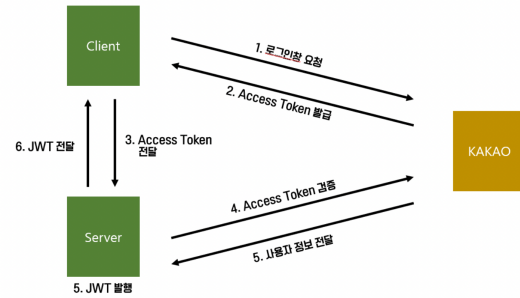
연동된 계정으로 로그인 시도 시, 서비스 제공자로부터 재확인이 완료되면, 이 과정이 바로 **소셜 로그인** (ID/PW 로그인이 아님.)



카카오 소셜 로그인 인증 방식

- 1. 클라이언트가 카카오로 로그인창을 요청

- 2. 클라이언트가 카카오로부터 access token 을 발급 받음
- 3. 발급 받은 access token 을 서버에 전달하면
 서버는 발급받은 access token을 다시 카카오에 검증 요청한다.
- 4. 카카오 서버는 클라이언트에게 발급 해준 토큰과 서버로부터 받은 토큰이 같을 경우, 사용자 정보를 내어준다.




카카오 소셜 로그인 Flow

카카오 API 사용할 수 있는 문서

Kakao Developers

이 문서는 카카오 로그인 및 관련 기능을 소개합니다. 카카오 로그인
 카카오계정으로 다양한 서비스에 로그인할 수 있도록 하는 OAuth 2.0
 기반의 소셜 로그인 서비스 입니다. 카카오 로그인 사용 시, 서비스는

 [https://developers.kakao.com/docs/latest/ko/kakaologin/com
mon](https://developers.kakao.com/docs/latest/ko/kakaologin/common)

kakao developers



카카오 소셜 로그인 Flow (백엔드가 해야 할 부분 → 3번, 4번)

- ▼ 1. 카카오가 프론트측으로 인가코드를 발급해준다.
- ▼ 2. 프론트측에서 인가코드를 통해 카카오에게 리프레시토큰, 액세스토큰을 받는다.
- ▼ 3. 백엔드가 프론트에게 액세스 토큰을 받는다.
- ▼ 4. 백엔드는 카카오측으로 액세스 토큰을 통해 user의 정보를 받아온다.
사용자 정보 가져오기

⚠ 동의 항목 설정 필요

이 API를 사용하려면 **동의 항목 설정**을 참고하여 필요한 사용자 정보 동의 항목을 설정해야 합니다. 동의 항목이 설정되어 있더라도 사용자가 **동의**하지 않으면 사용자 정보를 받을 수 없습니다. **동의 내역 확인하기** API를 통해 사용자가 동의한 동의 항목을 먼저 확인할 수 있습니다.

현재 로그인한 사용자의 정보를 불러옵니다. 사용자 정보 요청 REST API는 사용자 액세스 토큰을 사용하는 방법, 앱 어드민 키를 사용하는 방법 두 가지로 제공됩니다. 어드민 키는 보안에 유의하여 사용해야 하므로 서버에서 호출할 때만 사용합니다.

사용자 액세스 토큰 또는 어드민 키를 헤더(Header)에 담아 **GET** 또는 **POST** 로 요청합니다. 어드민 키로 요청할 때는 어떤 사용자의 정보가 필요한지 명시하기 위해 대상 사용자의 회원번호를 함께 전달합니다. 추가 파라미터를 사용하면 특정 정보만 지정해서 받아오거나 URL 응답 값을 **HTTPS** 로 받을지 지정할 수 있습니다.

사용자 정보에는 [내 애플리케이션] > [사용자 프로퍼티] 메뉴에서 설정한 **사용자 프로퍼티**가 포함됩니다.

사용자 정보 요청 성공 시, 응답 바디(Body)는 **JSON** 객체로 **사용자 정보**들을 포함합니다.

- user의 정보 요청을 성공하면, 응답 body는 Json 객체로 사용자 정보들을 포함
카카오가 토큰을 통해 사용자의 정보를 json 형태로 전달해주기 때문에 정보중에 원하는 것만 잘 사용하면 된다.

> Request

액세스 토큰 사용

URL

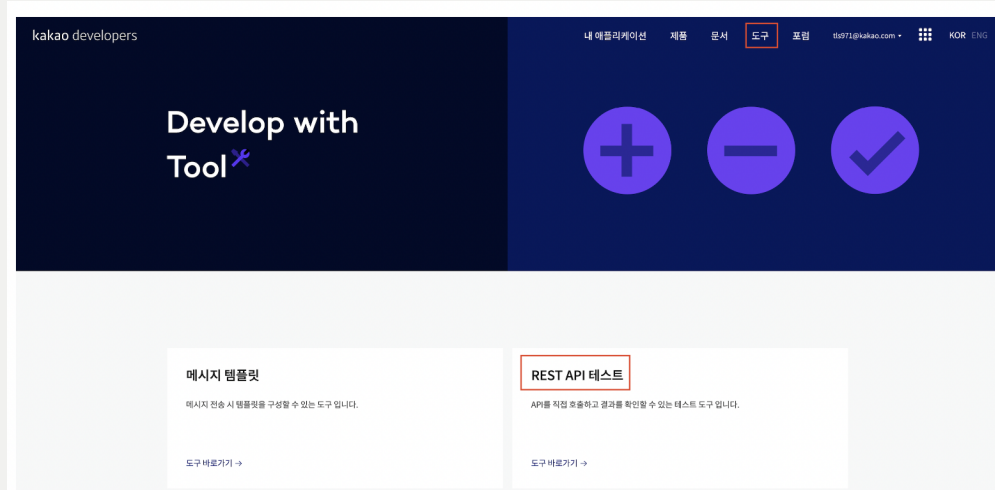
```
GET/POST /v2/user/me HTTP/1.1
Host: kapi.kakao.com
Authorization: Bearer {ACCESS_TOKEN}
Content-type: application/x-www-form-urlencoded;charset=utf-8
```

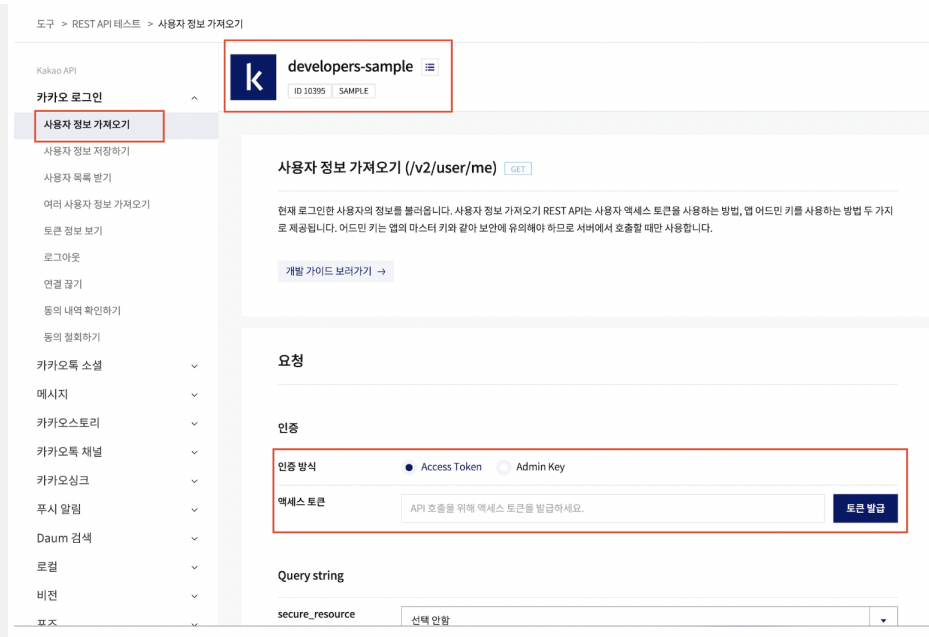
Header

Name	Description	Required
Authorization	사용자 인증 수단, 액세스 토큰 값 Authorization: Bearer {ACCESS_TOKEN}	O

1. GET/POST → method 이다, get,post 둘다 사용할 수 있다는 뜻
2. /v/user/me → 두번째 줄에 있는 Host 뒷 부분에 붙는 url
3. Authorization, Content-type → headers에 담아야 하는 부분

도구-REST API 테스트





developer-sample에서 본인이 등록한 애플리케이션으로 들어가야 한다

▼ 토큰정보

구분	설명	만료 시간
엑세스 토큰 (Access token)	사용자를 인증하고 카카오 API 호출 권한을 부여합니다.	Android, iOS : 12시간 JavaScript: 2 시간 REST API : 6시간
리프레시 토큰 (Refresh token)	일정 기간 동안 다시 인증 절차를 거치지 않고도 액세스 토큰 발급을 받을 수 있게 합니다. 유효한 리프레시 토큰이 있다면 사용자가 매번 카카오계정 정보를 입력하거나 카카오톡으로 로그인하지 않고도 액세스 토큰을 다시 발급받을 수 있습니다.	2달 만료 시간 1달 남은 시점부터 갱신 가능
ID 토큰 (ID token)	카카오 로그인 사용자의 인증 정보를 제공하는 토큰 자세한 정보는 OpenID Connect 참고	엑세스 토큰과 동일

- **Access Token** : HTTP Request의 authorization 헤더에 넣은 토큰, 일반적으로 JWT 형식사용 , 토큰은 분실의 위험이 있기때문에 보통 30분-1시간의 짧은 유효기간을 가진다.
- **Refresh Token** : 새로운 액세스 토큰을 얻을 수 있는 장기토큰(long lived token)보통은 특정 리소스를 위한 액세스 토큰을 얻는다.
(audience) 리프레시 토큰을 안전하게 사용할 수 있는 클라이언트만이 리프레시 토큰을 사용해야 함

- **ID Token** : 유저의 ID일반적으로 JWT 형식, ID 토큰은 절대 인증정보나 어떠한 리프레시 토큰 정보(audience information)를 가지고 있으면 안된다. 유저ID는 단순히 사용자를 구분(identify)하기 위해 사용한다.

Service Client

Service Server

Kakao Auth Server

인가코드 받기

1. 클라이언트 측에서 서비스 서버에 로그인 요청
2. 카카오 서버로부터 인가 코드 받기를 요청 → GET /oauth/authorize
3. 카카오 인증 서버가 클라이언트에게 카카오계정 로그인을 통한 인증을 요청
4. 클라이언트가 카카오계정으로 로그인
5. 카카오 인증 서버가 사용자에게 동의 화면을 출력하여 인가를 위한 사용자 동의를 요청함
6. 카카오 인증 서버는 서비스 서버에게 서비스 앱의 Redirect URI로 인가 코드를 전달

토큰 받기 → 인가코드 받은 뒤 액세스 토큰과 리프레시 토큰을 발급 받음

1. 서비스 서버에서 Redirect URI를 통해 전달받은 인가 코드로 카카오 인증 서버에게 토큰 받기를 요청 → Post /oauth/token
 - ✓ 필수 파라미터 값을 담아 Post로 요청
 - ✓ 요청 성공 시 응답은 Json 객체로 Redirect URI에 전달
 - ✓ 사용자가 로그인에 성공하면 액세스 토큰과 리프레시 토큰을 가짐
2. 카카오 인증 서버가 토큰을 발급하여 서비스 서버에 전달



무엇을 주고 무엇을 받아야하는지 →

프론트: 1. 카카오로부터 **인가코드**를 요청하고 카카오로부터 받은 인가코드를 백엔드에 넘겨줌,
2. 백엔드에서 전용토큰을 받아서 로그인 과정이 끝나면 이용할 수 있게 화면 전환

백엔드: 1. 프론트로부터 인가 코드를 넘겨받고 카카오 서버에게 인가코드로 토큰을 요청하여 토큰을 발급 받는다(유효성 검증),
2. 해당 토큰에 담긴 유저 정보를 활용해 프로젝트 전용(우리 서버 전용) 토큰으로 새롭게 발급 후 프론트에게 돌려준다

리프레시 토큰 액세스 토큰 두개 모두 db에 저장,

JWT 쿠키에 토큰 저장

카카오는 액세스 (짧은) 리프레시(두달 만료), 액세스는 L 저장할 필요없고 리프레시 저장 액세스가 만료됐으면 리프레시 주라고 요청 우리는 리프레시 주고 앱에서 만료되었다고 유저에게 알려줌 리프레시 토큰을 받아서 우리에게 줌

리프레시 토큰 어떻게 진행하는지 → 백엔드에서 인가코드로 카카오 서버에게 토큰 요청 , 유효성 검증 후(redirect URI 일치) 카카오 서버에서 토큰을 발급하여 서버에게 전달

누가 토큰을 발행 → 카카오 서버

카카오에 뭘 요청 → 1. 프론트에서는 카카오에게 인가코드를 요청, 2. 백엔드에서는 인가코드로 토큰 받기 요청