

인증의 오아시스, OIDC를 아시나요?

문성혁

Devops Engineer

데브시스터즈/AUSG

<https://github.com/roeniss>

예상 청자

- “새 프로젝트? 회원가입 form 만들게요!”
- “헉 보안 이슈... 백로그에 넣고 생각해야지”
- “SSO는 SAML 외엔 답이 없는 것 같은데?”

ID/PW 기반의 회원가입만 구현해본 분
자꾸 보안의 부담스런 시선을 피하는 분
OIDC를 조금만 맛보고 싶으신 분

지금까지의 방식, 뭐가 문제인가

지금까지의 방식, 뭐가 문제인가 (1/2)

예시 1: GitHub Actions

- `{{ secrets.ACCESS_KEY }}`, `{{ secrets.SECRET_KEY }}` in `workflow.yaml`
- “깃헙이 안전하게 숨겨준다” != “평생 재사용해도 된다”
 - 주기적인 키 로테이션은?
 - 권한 추적은?

⇒ 더 안전하고 감시하기 쉬운 방법이 필요하다

지금까지의 방식, 뭐가 문제인가 (2/2)

예시 2: 사내 서비스 인증 시스템의 파편화

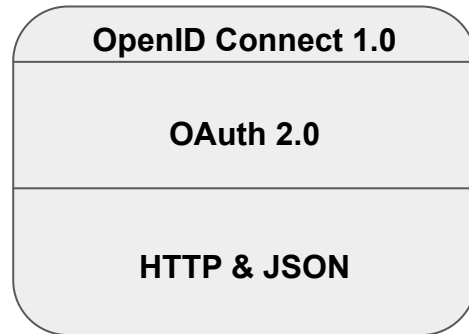
- 점점 늘어나는 서비스들
 - App for End-User, Admin, Data Analytics, Another Admin, ...
 - CREATE TABLE USERS (...) x N?
- 구현하는 개발자에게 고통
 - 쓰는 유저들에게는 더더욱 고통

⇒ 더 확장성있고 일관되게 구현할 수 있는 방법이 필요하다!

OIDC의 세계에 놀러오세요

OIDC의 세계에 놀러오세요 (1/3)

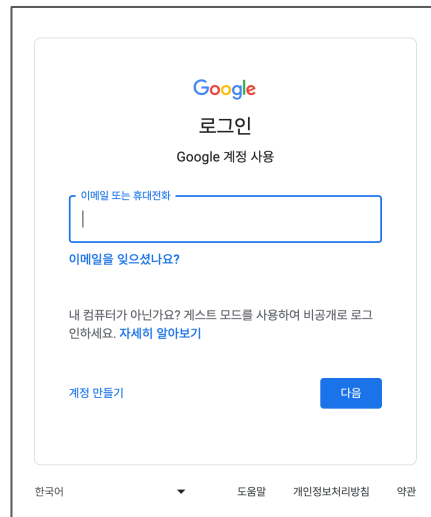
- "Authentication layer on OAuth 2.0"
 - OAuth 2.0의 Access Token은 누구의 토큰인지 설명하지 못함
- 간단한 특징들
 - ID token: 신원 증명서, JWT 포맷
 - Client ID & Secret : 나의 앱과 인증서버 간의 약속
 - Redirect URL: 콜백 주소
 - 여러가지 'Flow'



OIDC의 세계에 놀러오세요! (2/3)



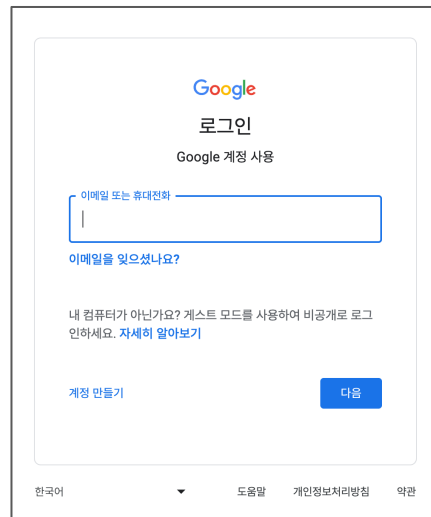
Hello
OIDC
Application

A screenshot of the Google login interface. At the top is the Google logo. Below it is the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). There is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone number). Below the input field is the text '이메일을 잊으셨나요?' (Forgot email?). There is a link '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Is it not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button '다음' (Next). At the very bottom, there is a language selector '한국어' (Korean) with a dropdown arrow, and links for '도움말' (Help), '개인정보처리방침' (Privacy policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

"똑똑. 앱 쓰고 싶어요"

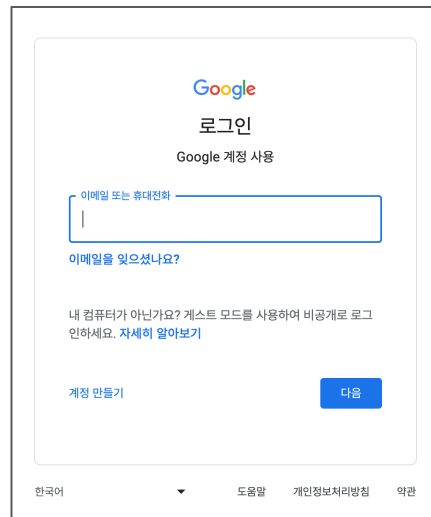
A screenshot of the Google login interface. At the top is the Google logo, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone). Under the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is a paragraph of text: '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application



"누구세요? 제 Identity Provider인
구글 가서 로그인하고 오세요"

A screenshot of the Google login interface. At the top is the Google logo, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone). Under the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is a link that says '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Is it not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

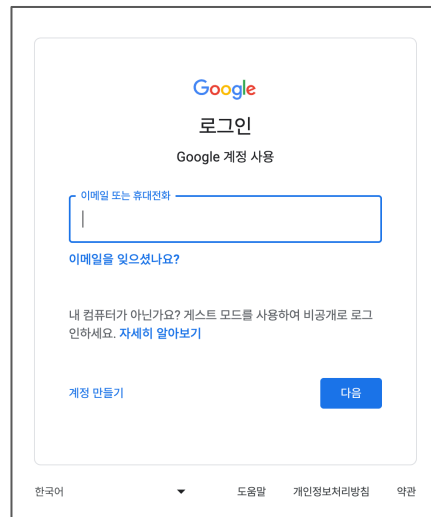
OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application



"이게 필요할 거예요"

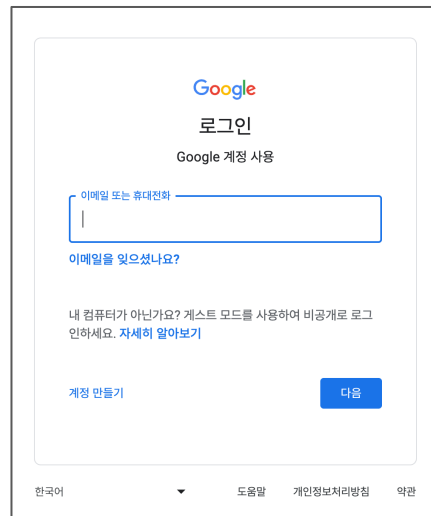
client_id=hello-oidc-app

A screenshot of the Google login interface. At the top is the Google logo. Below it is the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). There is a text input field for email or phone number. Below the field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is a link '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Is it not my computer? Sign in privately using Guest mode. Learn more). At the bottom are two buttons: '계정 만들기' (Create account) and '다음' (Next). The footer contains '한국어' (Korean), a dropdown arrow, '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

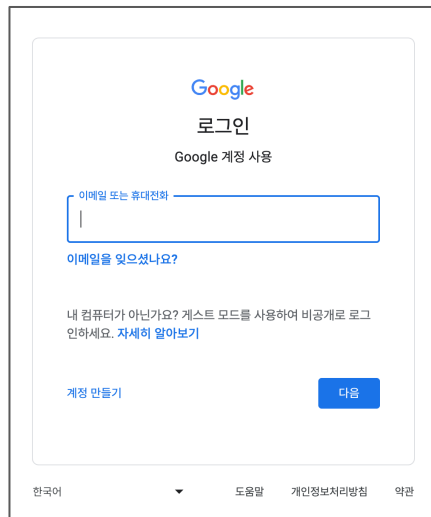
client_id=hello-oidc-app

A screenshot of the Google login page. At the top is the Google logo. Below it is the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). There is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone). Below the input field is the text '이메일을 잊으셨나요?' (Forgot email?). Further down is the text '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Not my computer? Sign in as a guest to keep your activity private. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button '다음' (Next). At the very bottom, there is a footer with '한국어' (Korean), a dropdown arrow, '도움말' (Help), '개인정보처리방침' (Privacy policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

client_id=hello-oidc-app

A screenshot of the Google login page. At the top is the Google logo, followed by the Korean text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone number). Under the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is the text '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

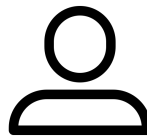
Hello
OIDC
Application

A screenshot of the Google login page. At the top is the Google logo, followed by the Korean text "로그인" (Login) and "Google 계정 사용" (Use Google Account). Below this is a text input field with the placeholder text "이메일 또는 휴대전화" (Email or phone). Under the input field is the text "이메일을 잊으셨나요?" (Forgot email?). Further down is a paragraph of text: "내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기" (Not my computer? Sign in privately using Guest mode. Learn more). At the bottom of the main content area are two links: "계정 만들기" (Create account) and a blue button labeled "다음" (Next). At the very bottom of the page are four links: "한국어" (Korean), a dropdown arrow, "도움말" (Help), "개인정보처리방침" (Privacy policy), and "약관" (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

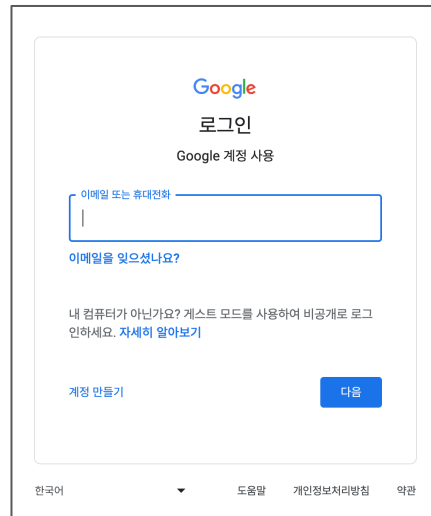
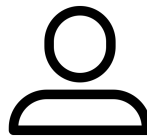
"안녕하세요 Seonghyeok!
client_id가 hello-oidc-app 군요.
이 client의 redirect_url 로 가시죠"

A screenshot of the Google login interface. At the top is the Google logo, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder '이메일 또는 휴대전화' (Email or phone). Under the input field is the text '이메일을 잊으셨나요?' (Forgot email?). Further down is a link '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

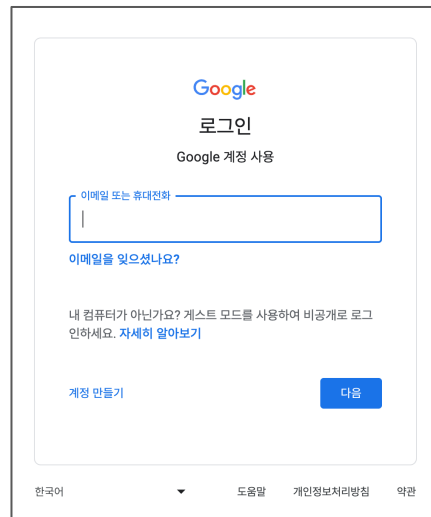
"이게 필요할 겁니다"
id_token

A screenshot of the Google login page. At the top is the Google logo, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder '이메일 또는 휴대전화' (Email or phone). Under the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is a link '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Is it not my computer? Log in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application


id_token



Google
로그인
Google 계정 사용

이메일 또는 휴대전화

이메일을 잊으셨나요?

내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. [자세히 알아보기](#)

[계정 만들기](#) [다음](#)

한국어 [도움말](#) [개인정보처리방침](#) [약관](#)

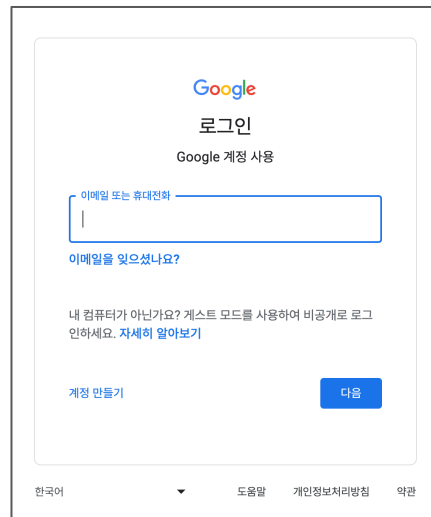
OIDC의 세계에 놀러오세요! (2/3)

Hello
OIDC
Application

"이제 들여보내주나요?"



id_token

A screenshot of the Google login page. At the top is the Google logo. Below it is the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). There is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone). Below the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). There is a link '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Is it not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요! (2/3)

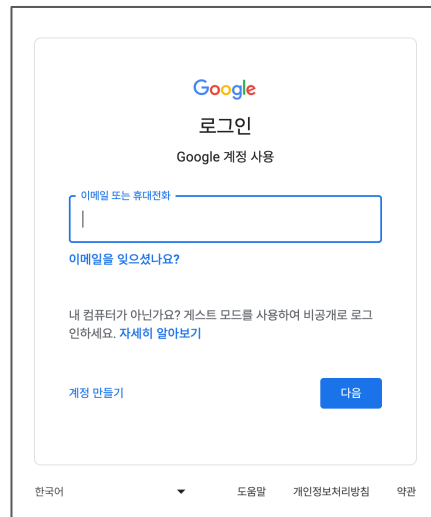
Hello
OIDC
Application



id_token

"id_token 좀 볼까요? 음..

오, Seonghyeok이군요!
어서 들어오세요."

A screenshot of the Google login page. At the top is the Google logo, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a text input field with the placeholder text '이메일 또는 휴대전화' (Email or phone). Under the input field is the text '이메일을 잊으셨나요?' (Forgot your email?). Further down is a paragraph of text: '내 컴퓨터가 아닌가요? 게스트 모드를 사용하여 비공개로 로그인하세요. 자세히 알아보기' (Not my computer? Sign in privately using Guest mode. Learn more). At the bottom left is a link '계정 만들기' (Create account) and at the bottom right is a blue button labeled '다음' (Next). At the very bottom of the page are links for '한국어' (Korean), '도움말' (Help), '개인정보처리방침' (Privacy Policy), and '약관' (Terms).

OIDC의 세계에 놀러오세요 (3/3)

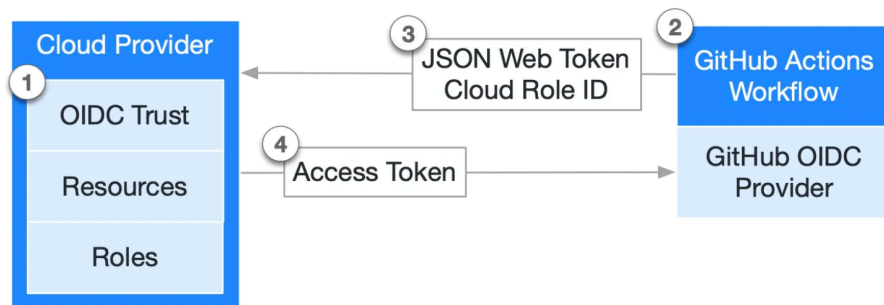
- "SAML로 충분하지 않나요?"
 - 그럼요! 그렇지만 OIDC는:
 - JWT
 - Mobile-friendly
 - AuthN + AuthZ

신나는 Demo 시간!

신나는 Demo 시간!

GitHub Actions + AWS

- IAM: Check Identity providers
- IAM: Create Role
- GitHub: Set role in workflow.yaml
- S3: Open static hosting url



요약하자면,

- OIDC 는 다른 인증 방식들에 비해 **더 안전하고, 확장성있고, 편리합니다**
 - 애플리케이션과 인증 서비스 사이의 신뢰 기반
 - 간단한 프로필 정보가 포함된 JWT 포맷의 ID token
 - 비 web 환경들도 원활하게 지원

Try it today!

흥미가 생기셨나요? 그렇다면...

- 조금 더 깊게 이해해보기

- https://openid.net/specs/openid-connect-core-1_0.html#StandardClaims
- <https://oauth.net/articles/authentication/#openid-connect>
- <https://auth0.com/intro-to-iam/what-is-openid-connect-oidc>
- <https://www.okta.com/identity-101/whats-the-difference-between-oauth-openid-connect-and-saml/>

- 실제로 적용해보기

- <https://docs.github.com/en/actions/deployment/security-hardening-your-deployments/about-security-hardening-with-openid-connect>
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_oidc.html
- <https://www.daleseo.com/google-oidc/>
- <https://developers.onelogin.com/openid-connect>