# SSO & ID federation 기술 @ IoT Platform

## - OpenID Connect, OAuth2 등 -


부산대학교

**김호원**

부산대
정보보호 및 IoT 연구실,
블록체인 보안 전문연구실,
사물인터넷연구센터


2018.11

# Gartner의 2019년 10대 전략 기술 트렌드

site: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/


## 가트너, 2019년 10대 전략 기술 트렌드 발표

[아이티데일리] 글로벌 IT 자문기관 가트너(Gartner)가 기업들이 주목해야할 2019년 주요 전략 기술 트렌드를 17일 발표했다.

가트너가 선정한 전략 기술 트렌드는 혁신적인 잠재력을 갖고 있는 기술들로 이뤄져 있다. 초기 상태에서 벗어나 보다 폭넓은 영향력과 활용 사례를 보이는 신기술과, 급성장세를 자랑하며 향후 5년 내 정점에 달할 것으로 예상되는 기술들이 이에 해당된다는 설명이다.

데이비드 설리(David Cearley) 가트너 부사장 겸 펠로우는 "지능(Intelligent), 디지털(Digital), 메시(Mesh)는 지난 2년 간 지속적으로 주목받았던 주제였으며, 2019년에도 주요 성장 요인으로 꼽힐 것이다. 이 세 가지 주제에 해당되는 트렌드들은 컨티뉴어스넥스트(ContinuousNEXT) 전략의 일환으로 지속적인 혁신 프로세스를 추진하는 핵심 요소"라고 말했다.

그는 "일례로, 자동화된 사물의 형태인 인공지능(AI)과 증강 지능(augmented intelligence)은 IoT, 에지 컴퓨팅, 디지털 트윈과 함께 이용돼 고도로 통합된 스마트 공간을 제공한다. 여러 트렌드들이 합쳐지면서 새로운 기회를 창출하고 새로운 혁신을 유도하는 종합적인 영향력은 가트너가 제시하는 2019년 10대 전략 트렌드의 특징"이라고 강조했다.

가트너가 제시하는 2019년 10대 전략 기술 트렌드는 다음과 같다.

**자율 사물(Autonomous Things)**
로봇, 드론, 자율주행차 등과 같은 '자율 사물'은 AI를 이용해 인간이 수행하던 기능들을 자동화한다. 이들이 제공하는 자동화는 엄격한 프로그래밍 모델을 통한 자동화의 수준을 뛰어 넘고, AI를 활용하여 주변 환경 및 사람들과 자연스럽게 상호작용하는 고급 행동을 선보인다.

데이비드 설리 부사장은 "자율 사물이 확산됨에 따라, 우리는 독립적인 지능형 사물에서 벗어나 인간의 명령을 따르거나 스스로 여러 디바이스들과 함께 작동할 수 있는 다양한 지능형 사물을 도입하게 될 것"이라며, "예를 들어, 드론이 넓은 밭을 조사해서 수확할 준비가 돼 있다는 결론을 내리면 '자율 수확기계'를 작동시키는 것이다. 혹은 배송 시장에서 가장 효율적인 해결책은 자율주행 차량을 이용해 소포들을 대상 지역으로 이동시키는 것이 될 수 있다. 차량에 탑재된 로봇과 드론은 소포의 최종 배송을 보장할 수 있다"고 설명했다.

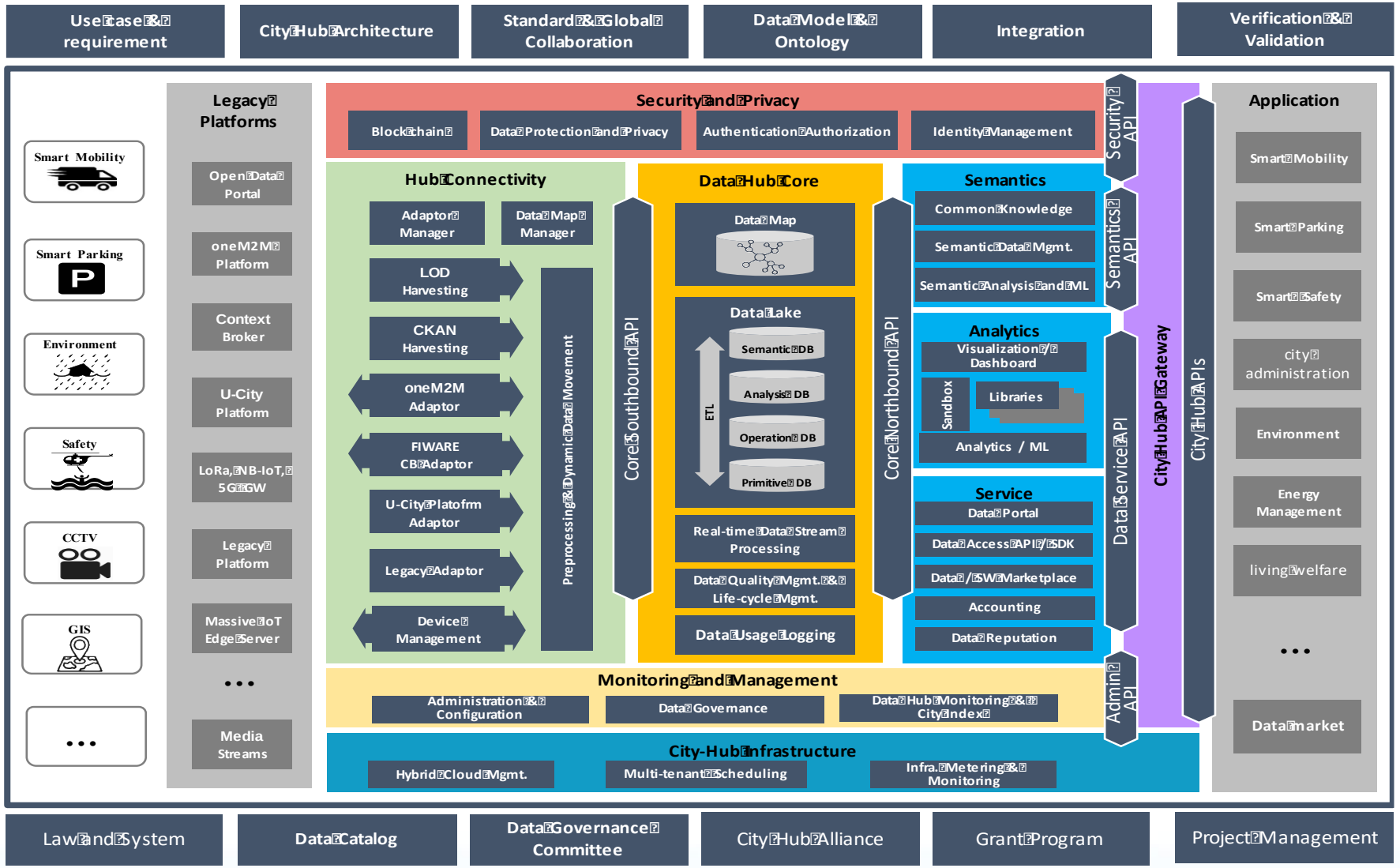
**증강 분석(Augmented Analytics)**
'증강 분석'은 분석 콘텐츠가 개발, 소비 및 공유되는 방식을 혁신하기 위해 머신러닝을 이용한 증강 지능의 특정 영역에 초점을 맞춘다. 증강 분석 기능은 데이터 준비, 데이터 관리, 최신 분석, 비즈니스 프로세스 관리, 프로세스 마이닝 및 데이터 사이언스 플랫폼의 주요 기능으로 빠르게 발전할 것으로 예상된다.

증강 분석으로부터 얻은 자동화된 통찰력은 HR, 재무, 영업, 마케팅, 고객 서비스, 구매조달 및 자산관리 부서 등의 기업 활동에 적용돼, 애널리스트나 데이터 과학자를 포함한 모든 직원들의 결정과 행동을 최적화할 전망이다. 증강 분석은 데이터 준비, 통찰력 생성 및 통찰력의 시각화 프로세스를 자동화해 많은 상황에서 전문 데이터 과학자가 필요하지 않게 된다.

데이비드 설리 부사장은 "이것은 통계나 분석 전문가가 아닌 사용자들도 데이터로부터 예측 혹은 규범적인 통찰력을 끌어낼 수 있도록 하는 새로운 역량 및 관행인 시민 데이터 과학(citizen data science)으로 이어질 것"이라며, "2020년까지 시민 데이터 과학자의 수는 전문 데이터 과학자의 수보다 5배 더 빠르게 증가할 것이다. 조직들은 시민 데이터 과학자들을 활용해, 데이터 과학자의 공급 부족과 높은 비용으로 야기된 데이터 사이언스 및 머신러닝 분야의 인력 부족 현상을 해소할 수 있을 것"이라고 말했다.

- 자율사물
- 증강분석
- 인공지능 주도 개발
- 디지털 트윈
- 자율권가진 에지
- 몰입 경험
- 블록체인
- 스마트공간
- 디지털윤리와 개인정보 보호
- 양자컴퓨팅

# City Hub 구조(KETI 스마트시티용 데이터 허브 구조 @2018.10)



# IoT 플랫폼에서의 SSO/ID federation 기술

## I. 개요

1. SAML/OAuth2/OpenID Connect

## II. OIDC(OpenID Interconnect)

1. 개요

## III. OAuth 2

1. 공개키 인증서 구조 및 원리

# I. Introduction

1. Single Sign On 정의
2. SAML/OAuth2/OpenID Connect

http://www.resilient-networks.com/concept-week-saml-oauth2-openid-connect/

# Single Sign-On 이란?

## Single sign-on

– allows user to be authenticated once, and applications can communicate with service to verify user's identity without repeatedly entering passwords

## Security Assertion Markup Language (SAML)

– standard for exchanging authentication and authorization information across security domains

- e.g. user from Yale signs on to external application such as acm.org using userid joe@yale.edu
- application communicates with Web-based authentication service at Yale to authenticate user, and find what the user is authorized to do by Yale (e.g. access certain journals)

## OpenID

– standard allows sharing of authentication across organizations

- e.g. application allows user to choose Yahoo! as OpenID authentication provider, and redirects user to Yahoo! for authentication

# 인증/인가 기술 - SAML, OAuth2, OpenID Connect

## Authentication(AuthN)/Authorization(AuthZ) techniqes

- Authentication is verifying that someone is who they claim to be
- Authorization is deciding which resources a user should be able to access, and what they should be allowed to do with those resources.

| | SAML 2.0 | OAuth2 | OpenID Connect |
|---|---|---|---|
| What is it? | Open standard for authorization and authentication | Open standard for authorization | Open standard for authentication |
| History | Developed by OASIS in 2001 | Developed by Twitter and Google in 2006 | Developed by the OpenID Foundation in 2014 |
| Primary use case | SSO for enterprise apps | API authorization | SSO for consumer apps |
| Format | XML | JSON | JSON |

## SAML (Security Assertion Markup Language)

- XML 기반. Two party 사이(특히 IP 제공자와 서비스 제공자 사이)에 인증/인가 데이터 전송에 활용됨
- Enterprise 응용에서 SSO 실현에 주로 사용됨
- 사용예: Google G Suite
- 단점 : mobile 이나 native app에는 부적함

https://nordicapis.com/api-security-oauth-openid-connect-depth/

# 인증/인가 기술 - SAML, OAuth2, OpenID Connect

## OAuth2

- Authorization 기능 제공. 소위 delegated access를 제공함. 즉, application은 사용자의 동의를 받고, application과 중요한 비밀정보를 공유하지 않고도 자원에 접근할 수 있도록 해줌
- 이는 identity provider가 3rd party application에 token을 발행함으로서 가능함
- 예로서, 3rd party app이 해당 사용자의 facebook 친구 리스트를 접하는 경우를 생각하면,
  - 먼저 사용자는 3rd party app에 있는 "facebook 친구 리스트 import" 단자를 클릭함
  - 사용자가 Facebook에 성공적으로 로그인하면, Facebook 친구 목록을 공유하라는 메시지가 표시됨
  - 사용자가 Yes를 클릭하면 3rd party app에 Facebook 친구 목록을 가져올 수 있는 권한과 승인을 부여하는 토큰과 함께 사용자는 app으로 돌아감
  - OAuth2는 사용자가 자격 증명을 공유하지 않고도 app에서 리소스에 액세스 할 수 있음
- 참고로 OAuth2는 인증 기능을 포함하지 않음

## OpenID Connect (OIDC)

- OAuth2와 함께 주로 사용됨. Authentication 기능 제공
- OAuth2 authorization flow에 identity token을 추가하여, end-user에 대한 기본 정보 제공/end-user 신원 확인에 사용됨
- OIDC는 mobile 기기와 native app에서 사용될 수 있는 구조 가짐 (인증/인가의 미래)
- 그래도 SAML은 enterprise 서비스에서 계속 존속 가능성 높음

# OpenID, OAuth2, SAML 비교

| | OAuth2 | OpenId | SAML |
|---|---|---|---|
| Token (or assertion) format | JSON or SAML2 | JSON | XML |
| Authorization? | Yes | No | Yes |
| Authentication? | Pseudo-authentication | Yes | Yes |
| Year created | 2005 | 2006 | 2001 |
| Current version | OAuth2 | OpenID Connect | SAML 2.0 |
| Transport | HTTP | HTTP GET and HTTP POST | HTTP Redirect (GET) binding, SAML SOAP binding, HTTP POST binding, and others |
| Security Risks | • Phishing 공격에 취약<br>• OAuth2는 서명, 암호화, 채널 바인딩, 클라이언트 검증 기능 제공하지 않음. 대신, TLS 기반으로 기밀성 제공함 | • Phishing 공격에 취약<br>• Identity providers는 OpenID 로그인에 대한 로그 기록을 모두 가짐. 만약 Identity Provider가 공격될 경우 Privacy 침해 문제 발생 | • XML Signature Wrapping to impersonate any user |
| Best suited for | API authorization | Single sign-on for consumer apps | Single sign-on for enterprise<br>Note: not well suited for mobile |

# Ⅱ. OIDC(OpenID Connect)

1. OIDC 개요
2. OIDC 프로토콜 절차

# What is OpenID Connect

- OIDC
  - Open, Decentralized single sign on standard
  - Allows users to use a single digital identity across multiple sites
  - Identity is represented by a URL or XRI

- Who supports OIDC ?
  - Yahoo
  - Google
  - AOL
  - VeriSign
  - BBC
  - Microsoft
  - LiveJournal.com
  - SourceForge.NET

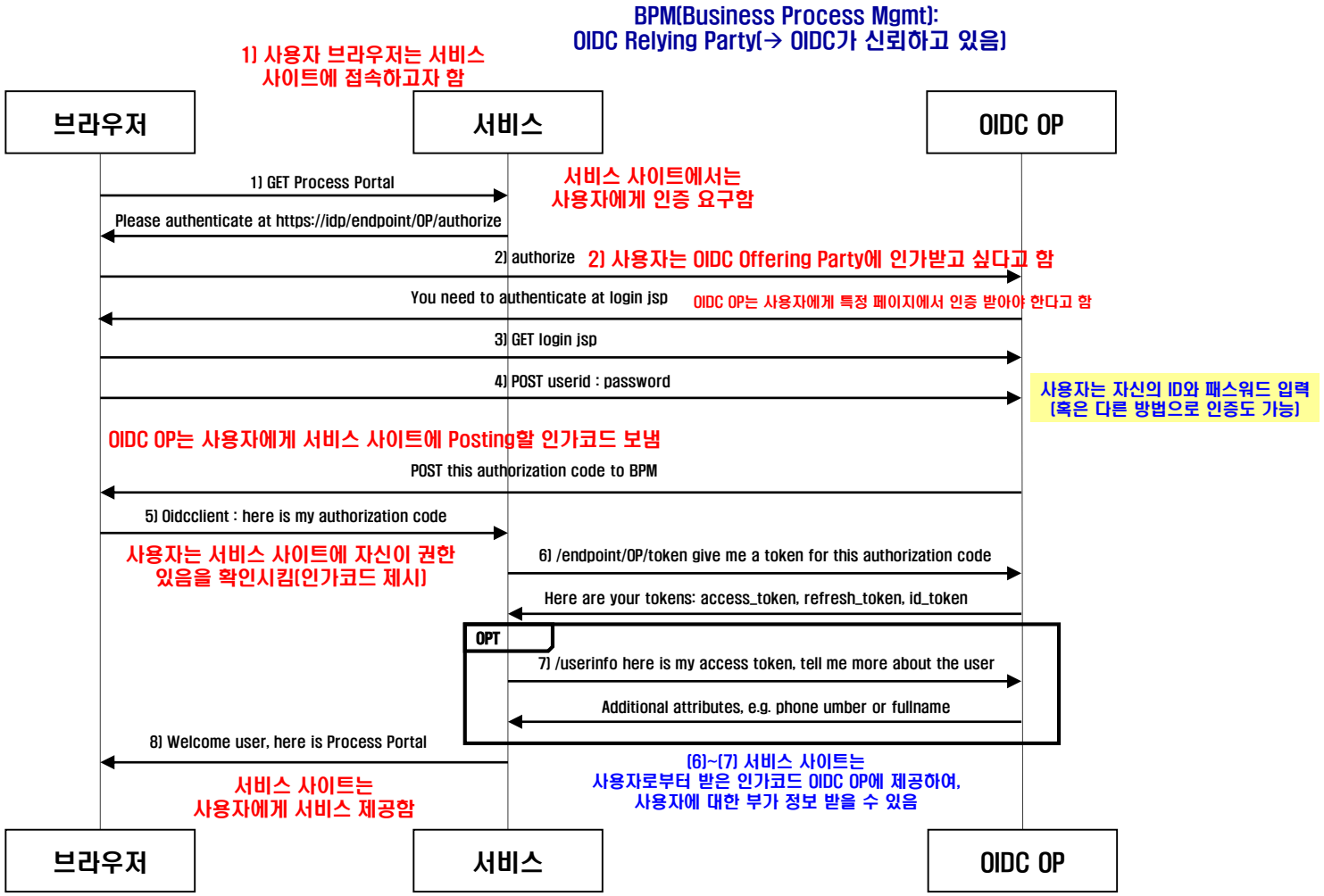
# Glossary of OIDC

## OIDC 주요 용어

- End-user
  - Person seeking to assert identity to a site
- Identifier
  - URL or XRI chosen by end-user
- Identity Provider₩OpenID Provider
  - Service provider who authenticates user and registers identifiers
- Relying Party (OIDC RP라고 함. OIDC가 신뢰하는 party)
  - Site seeking to authenticate End-user
- Server₩Server-Agent
  - Server verifying end-users identifier
- User Agent
  - Program used to access Identity provider or relying party
- eXtensible Resource Identifier (XRI)
  - Scheme and Resolution Protocol for Abstract  compatible with URI's

# OpenID Connect 프로토콜

## Open ID Connect 절차 Authentication Sequence




https://www.ibm.com/developerworks/community/blogs/d350350e-2c84-4d33-a25d-73b42c7fbb5e/resource/BLOGS_UPLOADED_IMAGES/AuthenticationSequence%281%29.png

# 참고 자료

## https://openid.net/developers/specs/


The Internet Identity Layer

OpenID Foundation | Intellectual Property | Current Working Groups
Specs & Dev Info | OpenID® Certification | OpenID Connect FAQ and Q&As
Workshops

Home » Developers » Specifications

# Specifications

OpenID specifications are developed by OpenID working groups and go through three phases: Drafts, Implementer's Drafts, and Final Specifications. Implementer's Drafts and Final Specifications provide intellectual property protections to implementers. Final Specifications are OpenID Foundation standards.

## Final Specifications

OpenID Connect specifications:

- OpenID Connect Core – Defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of claims to communicate information about the End-User
- OpenID Connect Discovery – Defines how clients dynamically discover information about OpenID Providers
- OpenID Connect Dynamic Registration – Defines how clients dynamically register with OpenID Providers
- OAuth 2.0 Multiple Response Types – Defines several specific new OAuth 2.0 response types
- OAuth 2.0 Form Post Response Mode – Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values that

Search

News Archives

Select Month

Categories

Select Category

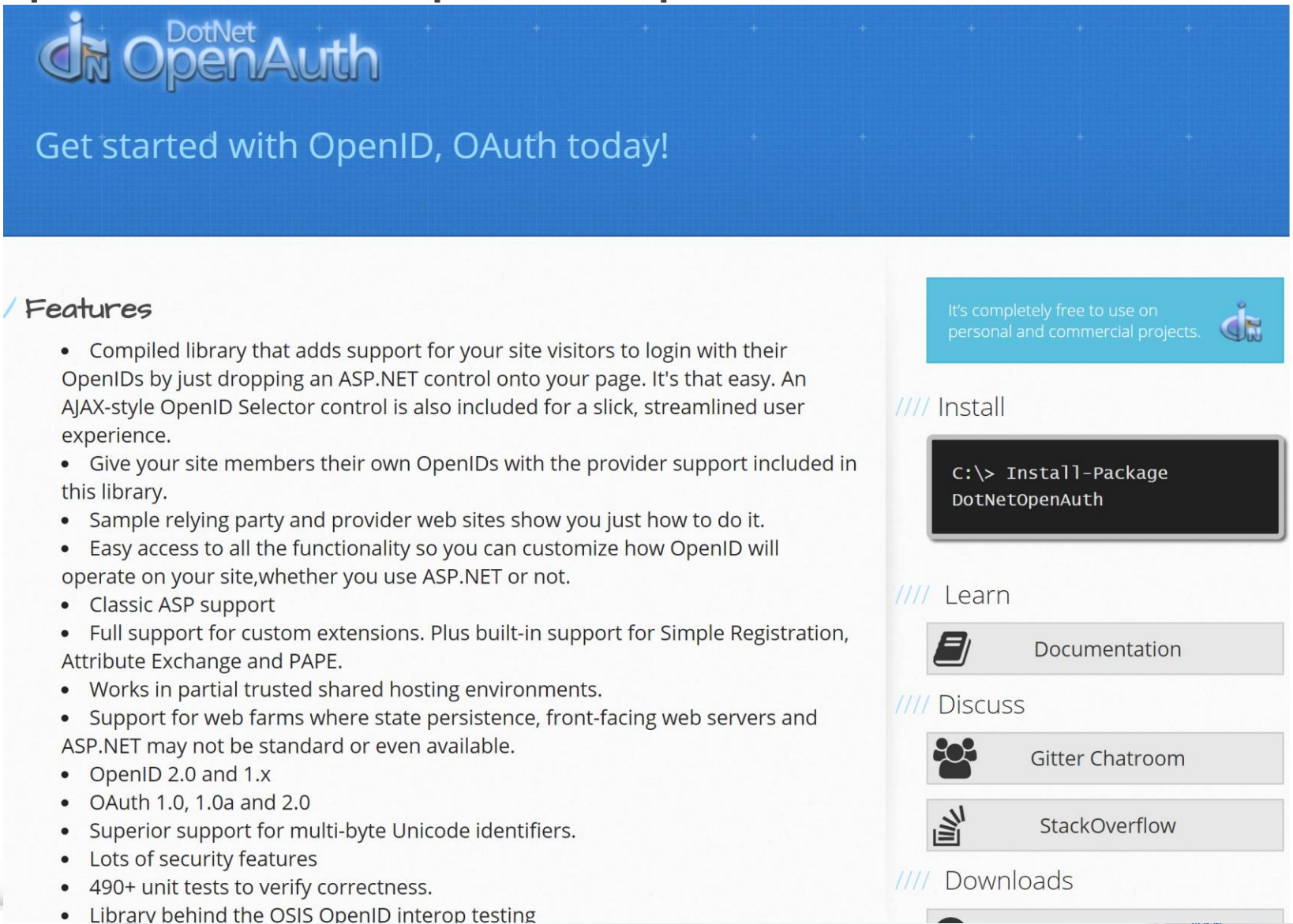
Recent Posts

› Implementer's Drafts of Three FAPI Specifications Approved

› Public Review Period for

# 참고 자료

## Open ID + OAuth - http://dotnetopenauth.net/



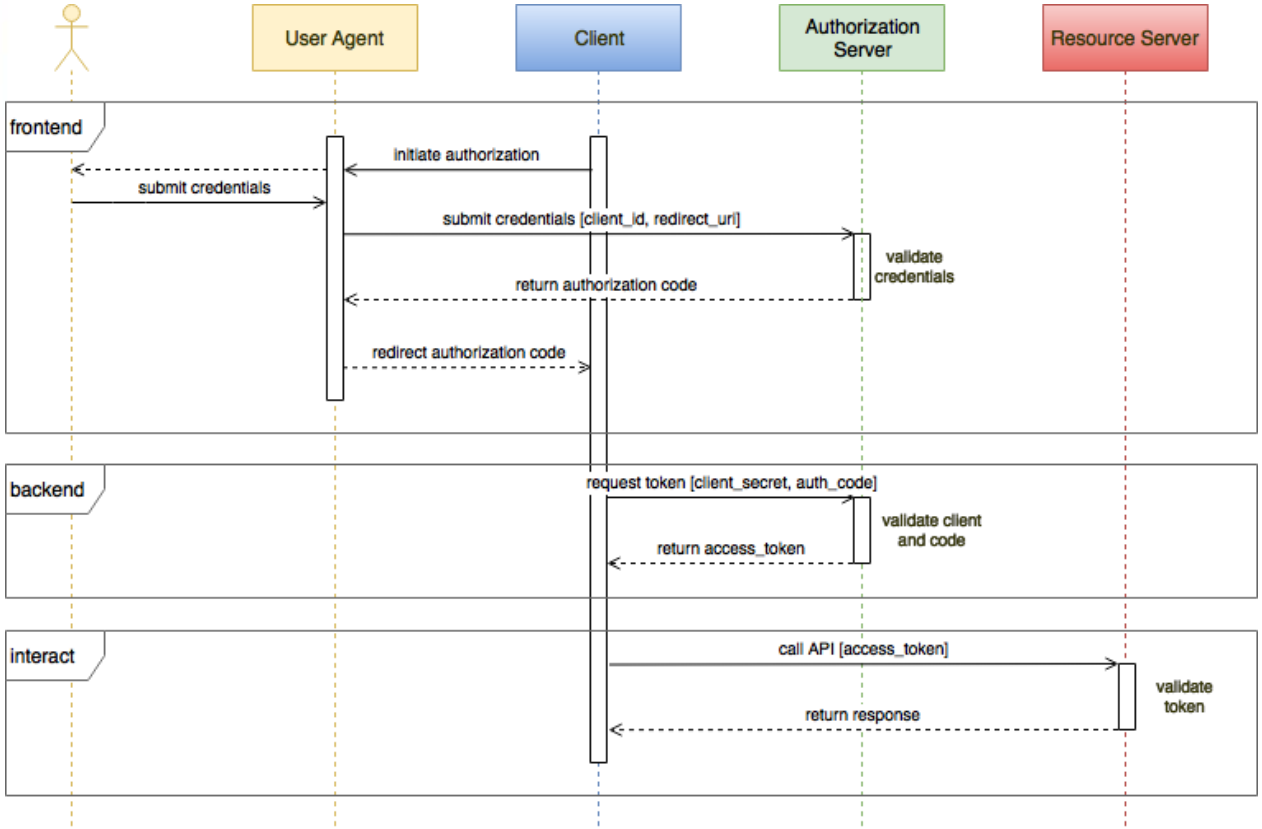
# Ⅲ. OAuth2

1. SAML/OAuth2/OpenID Connect

# OAuth2 프로토콜

## OAuth2 - detailed protocol

### – OAuth2 Authorization Code Grant Flow

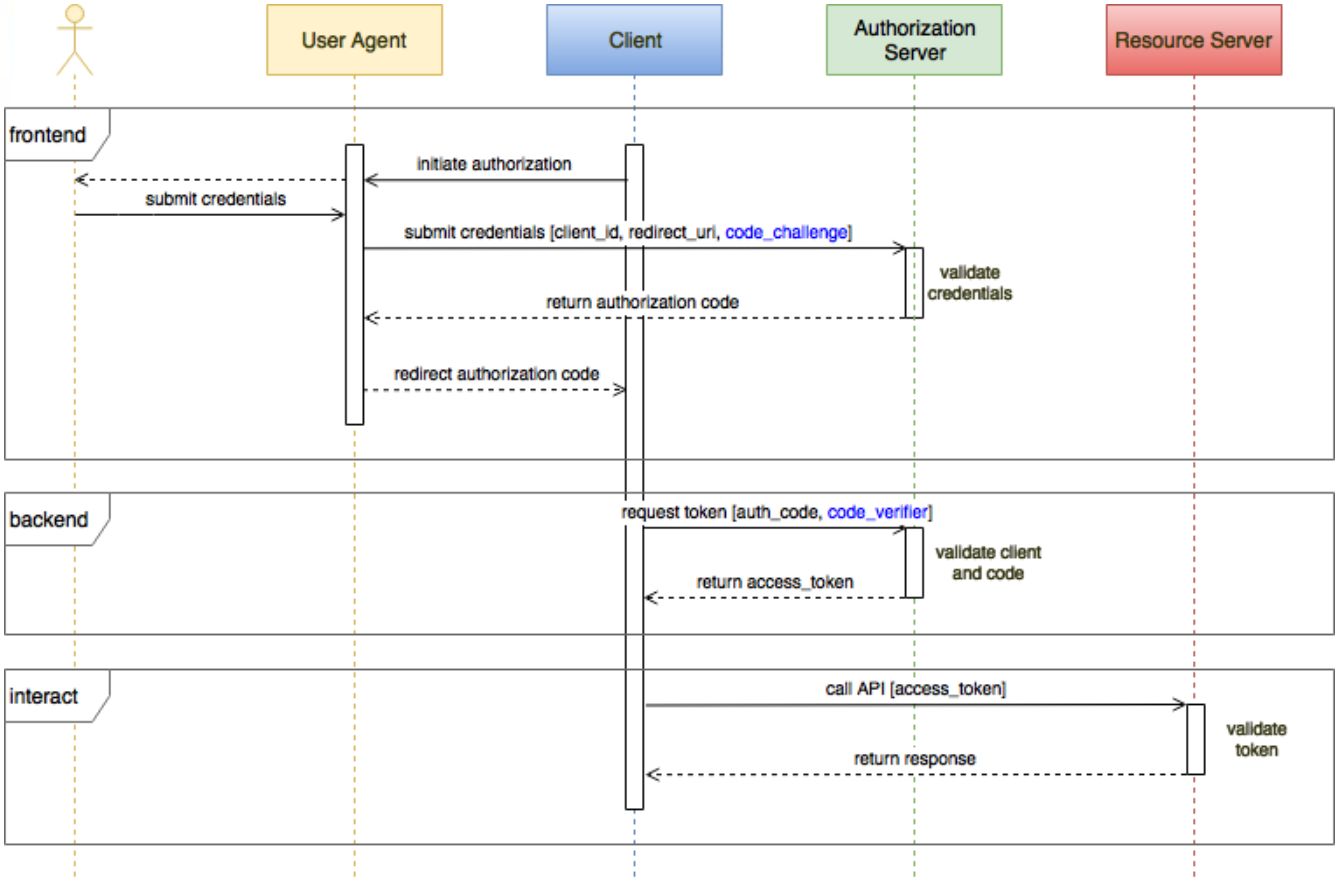



https://hackernoon.com/strengthening-oauth2-for-mobile-f4f3925dbf18

# OAuth2 프로토콜

## OAuth2 - detailed protocol

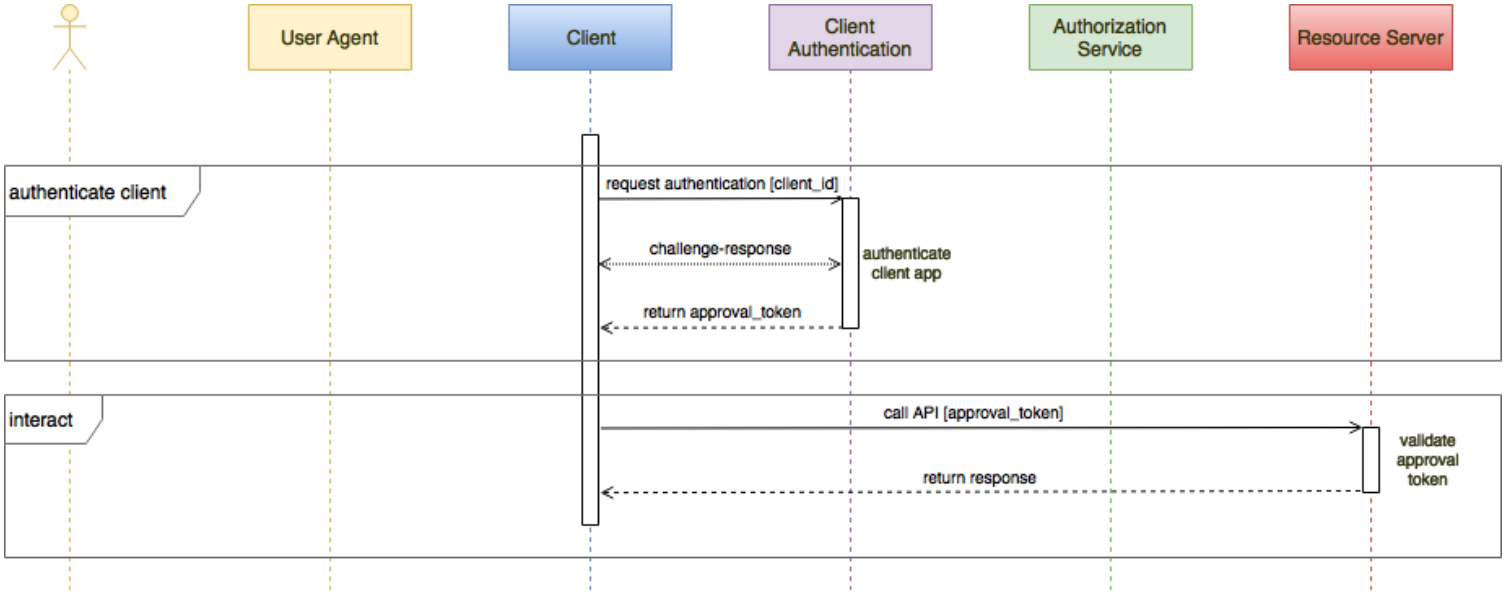
- OAuth2 Authorization Code Grant Flow with PKCE(Proof Key for Code Exchange)
- Static “client secret”의 위험성 대응




https://hackernoon.com/strengthening-oauth2-for-mobile-f4f3925dbf18

# OAuth2 프로토콜

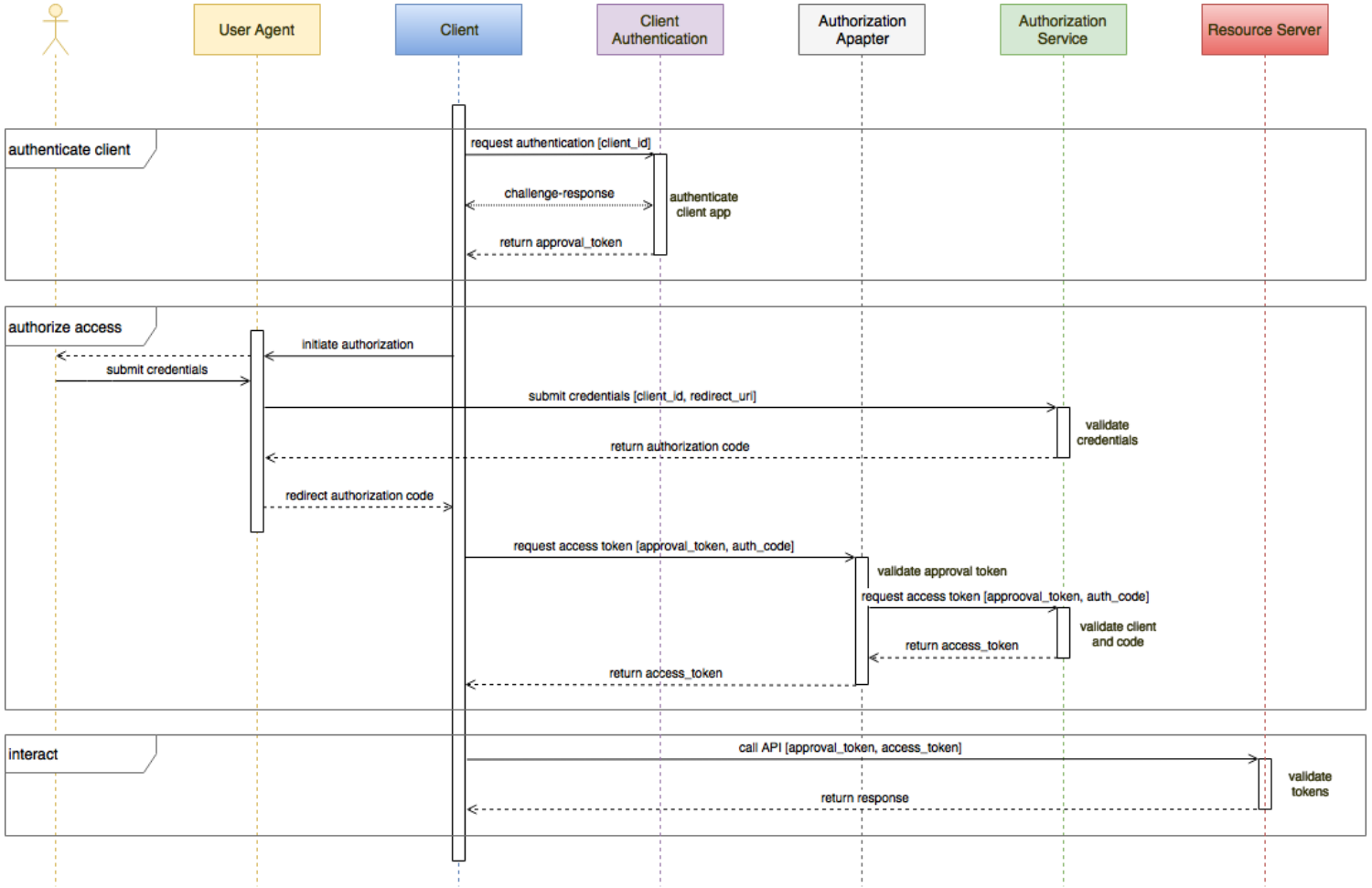
## Dynamic Client Authentication




https://hackernoon.com/strengthening-oauth2-for-mobile-f4f3925dbf18

# OAuth2 프로토콜

## Secure Mobile OAuth2 Code Grant Flow




https://hackernoon.com/strengthening-oauth2-for-mobile-f4f3925dbf18

# IV. API Security

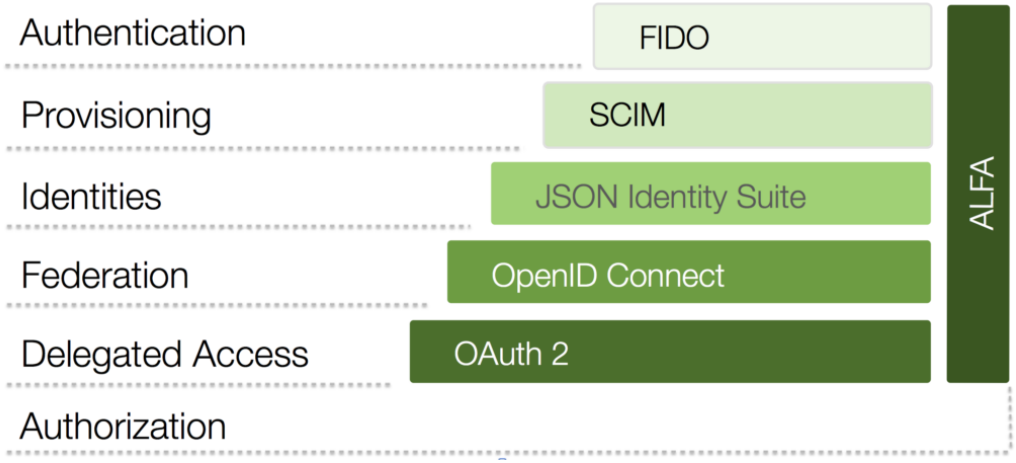
## Deep Dive into OAuth & OpenID Connect

https://nordicapis.com/api-security-oauth-openid-connect-depth/

# API 보안

## API 보안: Deep Dive into Oauth & OpenID Connect

- FIDO: Fast Identity Online - 온라인 환경에서 보다 편리하고 안전한 인증 시스템을 공동 구축하고 인증 시스템에 대한 기술 표준을 제시하는 역할 수행하는 연합체(alliance)
- SCIM 2.0: System for Cross-Domain Identity Management 기술(IETF 표준안) http://www.simplecloud.info/



# 감사합니다

# Q & A

부산대학교 전기컴퓨터공학부 김호원
부산대학교 사물인터넷 연구센터장
howonkim@pusan.ac.kr

# RSPF 프로토콜

## Integration