An Intro to OpenID Connect

Eugenio Pace - eugenio@auth0.com
30 min to...

OpenID Connect

- What is it?
- How it works?
- Why should you care?
OpenID Connect

A protocol used to authenticate users of an application, and represent those users in a standard way.
A typical (web) app

Application

Users

Database
Factoring out Auth

Application

Auth Server

Users
Factoring out Auth

Application

Auth Server

Users
Factoring out Auth
OIDC

Application
a.k.a. “Client”

Auth Server

Users

[Diagram showing the interaction between an Application (a.k.a. "Client") and an Auth Server, with a flow indicating users can be from various services like LinkedIn, Twitter, Facebook, and LDAP.]
OIDC

Application
a.k.a. “Client”

Auth Server

Users

{ id: 123, name: “john” }

LinkedIn
Twitter
Facebook
LDAP
How it works?

https://openidconnect.net
Authorization Code Flow - review

1. GET as/authorize? clientid=c1 redirect_uri=http://here/cb code=123

2. GET https://here/cb?code=123

3. POST as/token clientid=c1 clientsecret=shhhh code=123

Client “C1”
https://here

AS (or OP)

User agent (browser)

{ id: abc234
  name: “john”
}
id_token
OIDC & OAuth2

- OIDC is built on top of OAuth2
  - Same flows

- User information is encoded in an id_token

- OIDC = OAuth2 + JWT

- You can still get access_tokens to call APIs
Why?

- Industry standard:
  - Wide availability of SDKs, simplifies implementation
  - Interop: connect stuff with less effort
  - “Modern” ➔ lightweight / cloud friendly
  - Avoid lock-in
Why?

- **Industry standard:**
  - Wide availability of SDKs, simplifies implementation
  - Interop: connect stuff with less effort
  - “Modern” → lightweight / cloud friendly
  - Avoid lock-in

- **Standing on the shoulder of giants:**
  - Battle tested (e.g. Google, FB, and many many more)
  - Security proofed
Resources / Learn more

- **Standard:**
  - [http://openid.net](http://openid.net)
  - Core: [http://openid.net/specs/openid-connect-core-1_0.html](http://openid.net/specs/openid-connect-core-1_0.html)

- **OIDC Playground**
  - [https://openidconnect.net](https://openidconnect.net)

- **JWT Playground**
  - [http://jwt.io](http://jwt.io)

- **Overview of Protocols**
  - [https://docs.auth0.com/protocols](https://docs.auth0.com/protocols)
https://auth0.com