

# Whooooooooo Are You? I Really Want to Know... the Magic Behind OIDC

Eddie Zaneski  
@eddiezane

# Hi, I'm Eddie!



- Staff DevRel + OSS Engineer @chainguard\_dev
- @eddiezane
- Denver, CO
- Climb big mountains
- Maintainer for the Kubernetes and Sigstore projects
- **Not a Cryptographer or Security Engineer**

# Disclaimer

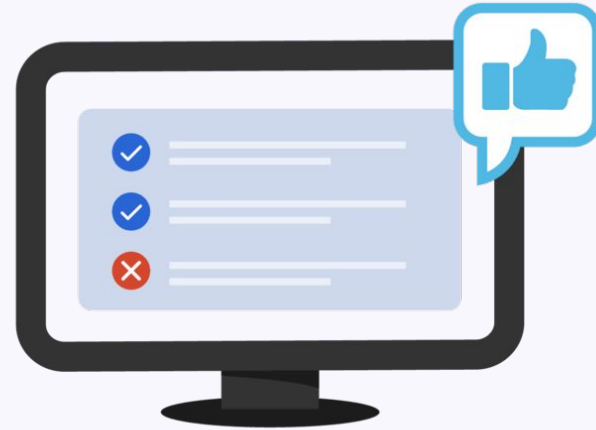
# **Authentication (AuthN) vs Authorization (AuthZ)**

## Authentication




Confirms users  
are who they say they are.

## Authorization



Gives users permission  
to access a resource.

okta

  
Real People. Real Reviews.™

Search for (e.g. taco, salon, Max's)

Near (Address, Neighborhood, City, State or Zip)  
San Francisco, CA


Search


WelcomeAbout MeWrite a ReviewFind ReviewsInvite FriendsMessagingTalkEventsMember


### Are your friends already on Yelp?


Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite. Don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service

☐  Hotmail

☐  YAHOO! MAIL


☐  AOL Mail

☐ 

Your Email Address  (e.g. bob@yahoo.com)

Your Yahoo Password  (The password you use to log into your Yahoo email)

[Skip this step](#)[Check Contacts](#)



[Business Owners](#) | [My Account](#) | [About Yelp](#) | [FAQ](#) | [The Weekly Yelp](#) | [Yelp Blog](#) | [Yelp Mobile](#) | [Yelp Canada](#) | [RSS](#) | [Developers](#) | [Feedback](#)

Use of this site is subject to express [Terms of Service](#). By continuing past this page, you agree to abide by these terms.

Copyright © 2004-2008 Yelp | [Privacy Policy](#)

[Site Map](#) | [Atlanta](#) | [Austin](#) | [Boston](#) | [Chicago](#) | [Dallas](#) | [Denver](#) | [Honolulu](#) | [Houston](#) | [Las Vegas](#) | [Los Angeles](#) | [Miami](#) | [New York](#) | [Philadelphia](#) | [Phoenix](#) | [Portland](#) | [San Francisco](#) | [San Jose](#) | [Seattle](#) | [Washington, DC](#) | [More Cities](#)

[Review Guidelines](#) | [Atlanta](#) | [Austin](#) | [Boston](#) | [Chicago](#) | [Dallas](#) | [Denver](#) | [Honolulu](#) | [Houston](#) | [Las Vegas](#) | [Los Angeles](#) | [Miami](#) | [New York](#) | [Philadelphia](#) | [Phoenix](#) | [Portland](#) | [San Francisco](#) | [San Jose](#) | [Seattle](#) | [Washington, DC](#) | [More Cities](#)

# OAuth 2.0

 Sign in with Google



## Choose an account

to continue to **Clockwise**



**Eddie Zaneski**

eddiezane@chainguard.dev



Use another account

To continue, Google will share your name, email address, language preference, and profile picture with Clockwise. Before using this app, you can review Clockwise's [privacy policy](#) and [terms of service](#).

English (United States) ▼

[Help](#)

[Privacy](#)

[Terms](#)

 Sign in with Google











## **Clockwise** wants to access your Google Account



eddiezane@chainguard.dev

This will allow **Clockwise** to:

-  View calendar resources on your domain 
-  See info about users on your domain 
-  See and download your contacts 
-  See, edit, share, and permanently delete all the calendars you can access using Google Calendar 

### Make sure you trust Clockwise

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See Clockwise's [Privacy Policy](#) and [Terms of Service](#).

[Cancel](#)

[Allow](#)





## OAuth Demo

You agree that OAuth Demo will be able to:

View your Spotify account data

Your email

Your name and username, your profile picture, how many followers you have on Spotify and your public playlists

You can remove this access at any time at [spotify.com/account](https://spotify.com/account).

For more information about how OAuth Demo can use your personal data, please see OAuth Demo's privacy policy.



Logged in as eddiezane.  
[Not you?](#)

AGREE

CANCEL



## Authorize Tailscale



Tailscale by Tailscale  
wants to access your eddiezane account

### Existing access

✓ Read org and team membership, read org projects

### Organization access

Angelbots1339 ✓

Denhac ✓

chainguard-dev ✕

kubernetes ✕

kubernetes-sigs ✕

RM-RedTeam ✕

sigstore ✕

kuberneddies ✕

Request

Request

Request

Request

Request

Grant

Cancel

Authorize tailscale

Authorizing will redirect to  
<https://login.tailscale.com>

Not owned or  
operated by GitHub

Created 2 years ago

More than 1K  
GitHub users

[Learn more about OAuth](#)

# OAuth 2.0

- Designed for Authorization (not Authentication)
- Resource Provider has a resource
- Flows
  - Authorization code
  - Client credentials
  - Device
  - Implicit
- Scopes
  - user-read-email
  - okta.users.read
  - <https://www.googleapis.com/auth/spreadsheets>
- [https://accounts.google.com/o/oauth2/v2/auth?client\\_id=482789919864-mrcrgilj9j20luus5bkdk7nib2cb5e1.apps.googleusercontent.com&redirect\\_uri=http://localhost:8080/callback&response\\_type=code&scope=openid+email+https://www.googleapis.com/auth/spreadsheets&state=foo](https://accounts.google.com/o/oauth2/v2/auth?client_id=482789919864-mrcrgilj9j20luus5bkdk7nib2cb5e1.apps.googleusercontent.com&redirect_uri=http://localhost:8080/callback&response_type=code&scope=openid+email+https://www.googleapis.com/auth/spreadsheets&state=foo)



## Demo App

Active ▾



View Logs

General

Sign On

Assignments

Okta API Scopes

### Client Credentials

Edit

Client ID

Ooa85s28lyHmutA7I5d7



Public identifier for the client that is required for all OAuth flows.

Client authentication



Client secret



Public key / Private key

Proof Key for Code Exchange (PKCE)



Require PKCE as additional verification

### CLIENT SECRETS

Generate new secret

Creation date	Secret	Status
Jan 30, 2023	.....	  Active ▾

### LOGIN

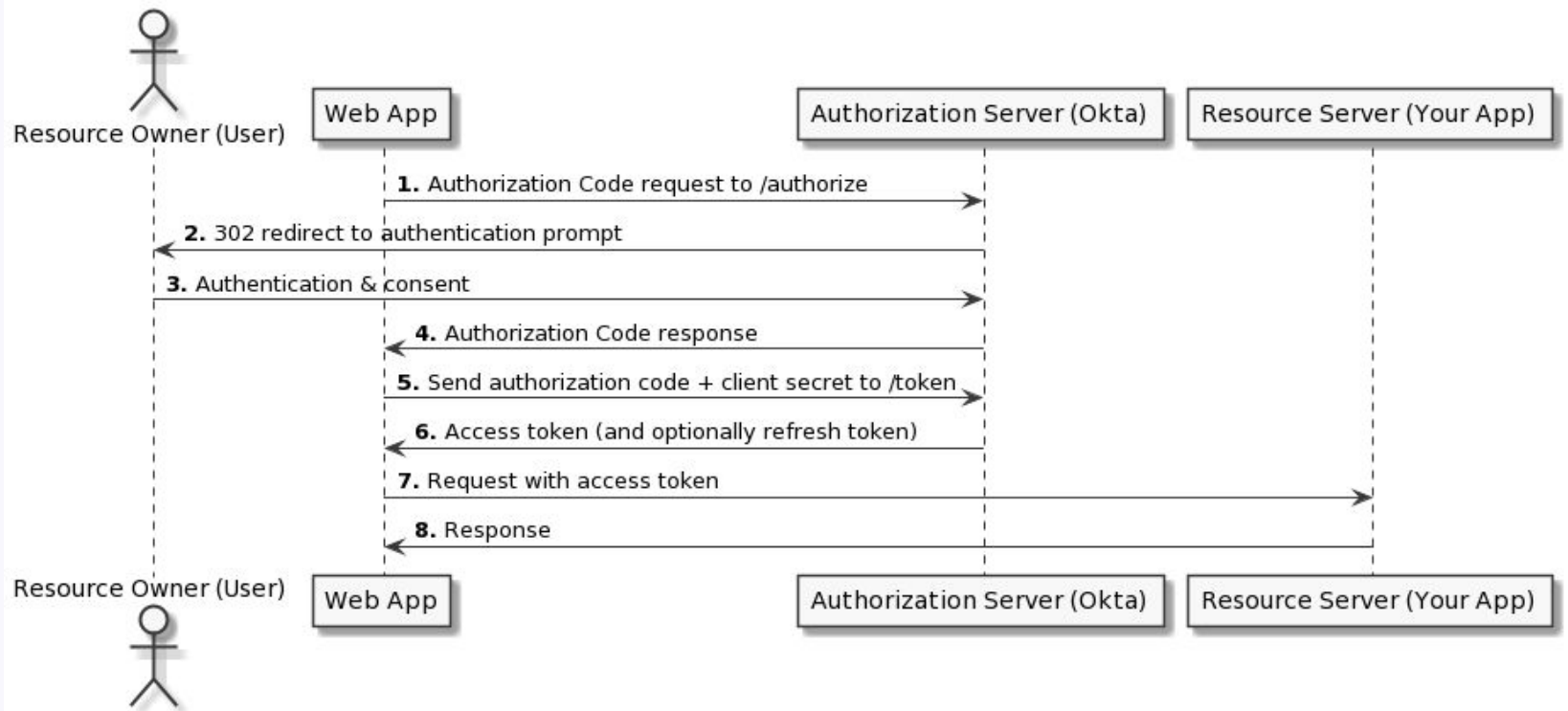
Sign-in redirect URIs ⓘ

☐ Allow wildcard \* in login URI redirect.

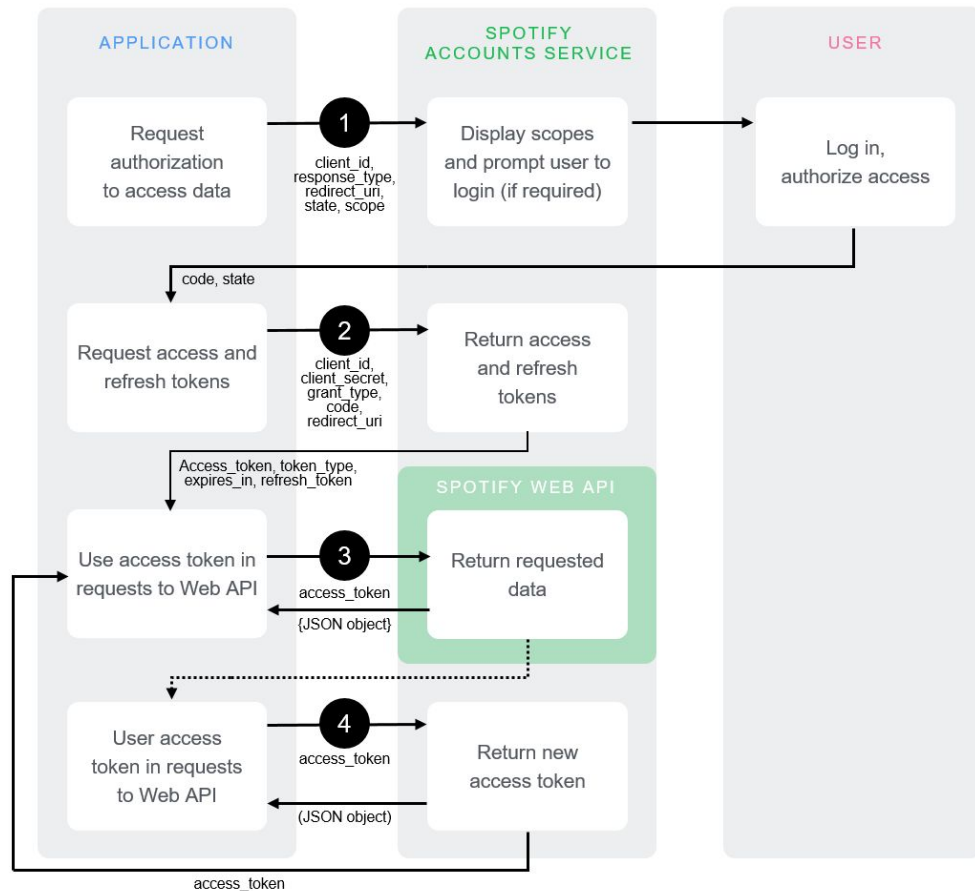
http://localhost:8080/authorization-code/callback

Sign-out redirect URIs ⓘ

http://localhost:8080



# Spotify Demo



# Gitsign Demo

## Issues With OAuth

- Developers wanted to use it for Authentication
- No standard scopes
- No standard whoami endpoint
- Long lived credentials
- Discovery?
  - <https://accounts.spotify.com/.well-known/oauth-authorization-server>



**Enter OIDC**

# OIDC

- OpenID Connect
- Extension to OAuth 2.0
- ID token (JWT)
- UserInfo endpoint
- Standard set of scopes
  - openid
  - profile
- Well known discovery

# JSON Web Token

- 3 sections
  - Header
  - Payload (claims)
  - Signature
- Claims
  - sub - client id
  - aud - auth server
  - iss - issuer of this token
  - iat - issued at timestamp
  - exp - expires at timestamp
- <https://jwt.io>
- step-cli

# Okta Demo

# OIDC Discovery

- Issuer
  - <https://accounts.google.com>
- /.well-known/openid-configuration
  - <https://accounts.google.com/.well-known/openid-configuration>
- jwks\_uri (JSON Web Key Set)
  - <https://www.googleapis.com/oauth2/v3/certs>
- JOSE (JSON Object Signing and Encryption)

# Federation

# Federation

- Trust relationship between issuer and resource provider
- No long lived credentials!
- Assume roles/identities for permissions
- Still auditable

## Where?

- CI/CD
  - GitHub/GitLab/CircleCI
  - Jenkins plugin
- Cloud resources
- [Kubernetes](#)
- Sigstore signing



```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "example-thumbprint",
  "kid": "example-key-id"
}
{
  "jti": "example-id",
  "sub": "repo:octo-org/octo-repo:environment:prod",
  "environment": "prod",
  "aud": "https://github.com/octo-org",
  "ref": "refs/heads/main",
  "sha": "example-sha",
  "repository": "octo-org/octo-repo",
  "repository_owner": "octo-org",
  "actor_id": "12",
  "repository_visibility": "private",
  "repository_id": "74",
  "repository_owner_id": "65",
  "run_id": "example-run-id",
  "run_number": "10",
  "run_attempt": "2",
  "actor": "octocat",
  "workflow": "example-workflow",
  "head_ref": "",
  "base_ref": "",
  "event_name": "workflow_dispatch",
  "ref_type": "branch",
  "job_workflow_ref": "octo-org/octo-automation/.github/workflows/oidc.yml@refs/heads/main",
  "iss": "https://token.actions.githubusercontent.com",
  "nbf": 1632492967,
  "exp": 1632493867,
  "iat": 1632493567
}
```

# GitHub Demo

# Kubernetes Demo

## OIDC Wave 2

- Standalone token issuer detached from OAuth
- GitHub Actions
- Machine Identity
- Who do you want signing releases?

## Trust But Verify

- Anyone can mint a token
- Claims matter
- iss, sub, aud
- What happens if a service were to issue whatever?

<https://justtrustme.dev>

# AWS + GCP Demo

# Protection

- Verify token and claims
- Pass audience alongside token
  - <https://cloud.google.com/iam/docs/reference/sts/rest/v1/TopLevel/token>



## What else?

- Dex
  - Portal to other apps
  - Used with Sigstore
- SPIFFE/SPIRE

# Thanks!

Questions?

@eddiezane

