



# The Software Engineer's Guide to Public APIs

Scott McAllister

@stmcallister

## Titanium Sponsors

okta

Headspring

## Platinum Sponsors

PAiGE  
TECHNOLOGIES  
INTELLIGENT PAIRING. PERPETUAL SUCCESS.

EVENT STORE.

Homebase

Dimensional  
Innovations

WellSky

DevExpress®

Progress® Telerik®

AxonIQ

Algorand

smg  
service  
management  
group®

Red Hat

NAIC  
National Association of Insurance Commissioners

NIPR  
NATIONAL INSURANCE  
PRODUCER REGISTRY

SAUCELABS

Veterans United.  
Home Loans

ROCKET  
Companies

trility®

JOHN DEERE

ascend  
LEARNING

Mattermost

## Gold Sponsors

touchnet  
A Global Payments Company

Advantage  
Tech  
IT Staffing &  
Recruiting Services

pk prokarma

ORION

TEAM Software

Netsmart

BUILDERTREND

Cerner

VMLY&R

ARTISAN  
TECHNOLOGY GROUP

Leggett & Platt.

QUEST  
ANALYTICS

MOONSHOT  
INNOVATIONS

SHAMROCK™  
TRADING  
CORPORATION

SETWorks

# Why APIs? Because every business is a Digital Business and they communicate via APIs

Make payments



Get around



Do work



Buy anything



Stay healthy



Shop online



Be entertained



Order food



Be connected



# What is an API?

Messenger that sends and receives requests for an application





# API Standards

## *HTTP*

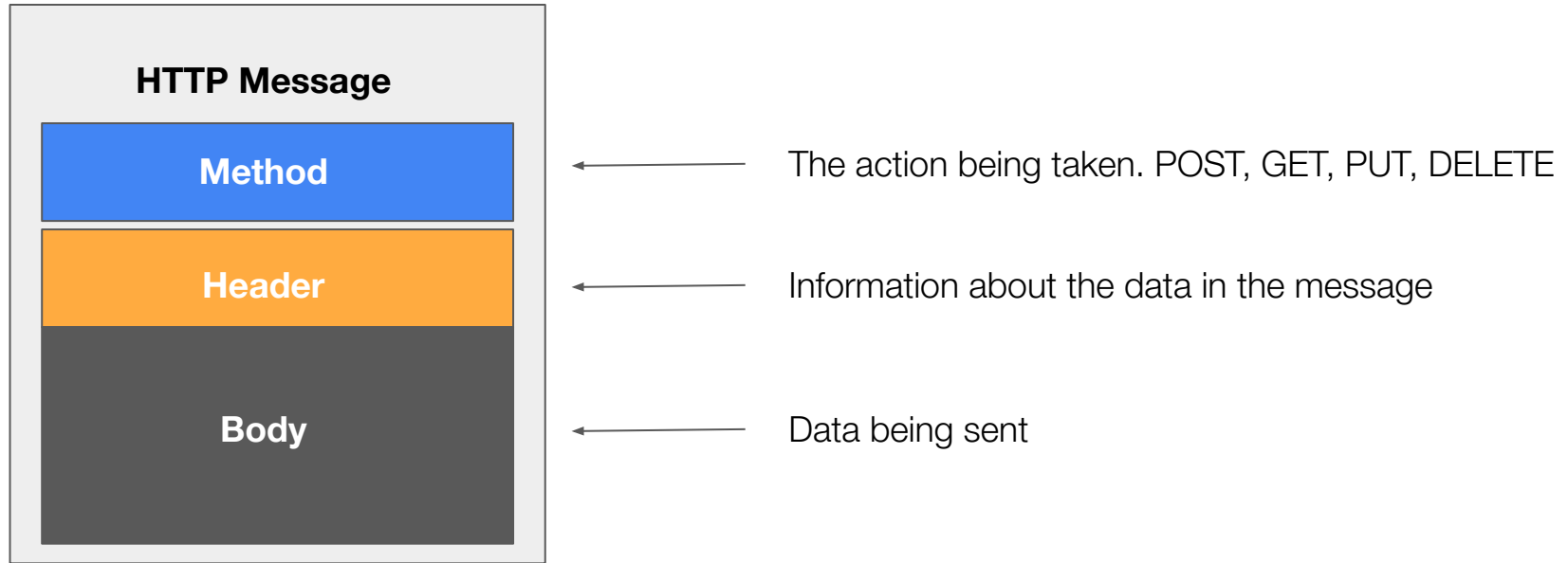
**POST** → **Create** data

**GET** → **Read** data

**PUT** → **Update** data

**DELETE** → **Delete** data

# HTTP Messages



# Authorization Header

Contains the API token which is required to authenticate and authorize each request with API

```
Authorization: Token token=w_8PcNuhHa-y3xYdmc1x
```

# Authentication

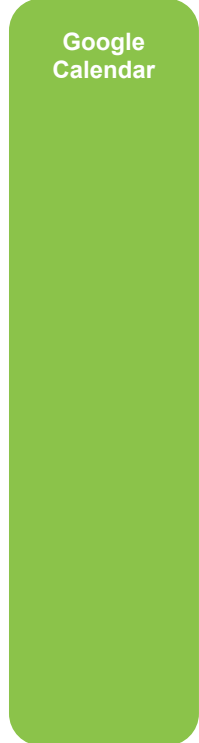
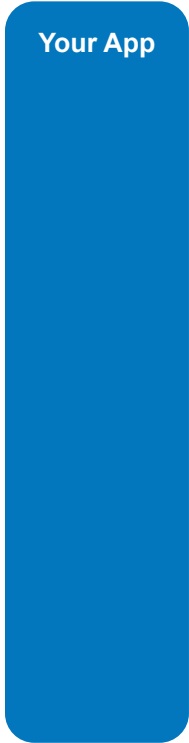
## OAuth

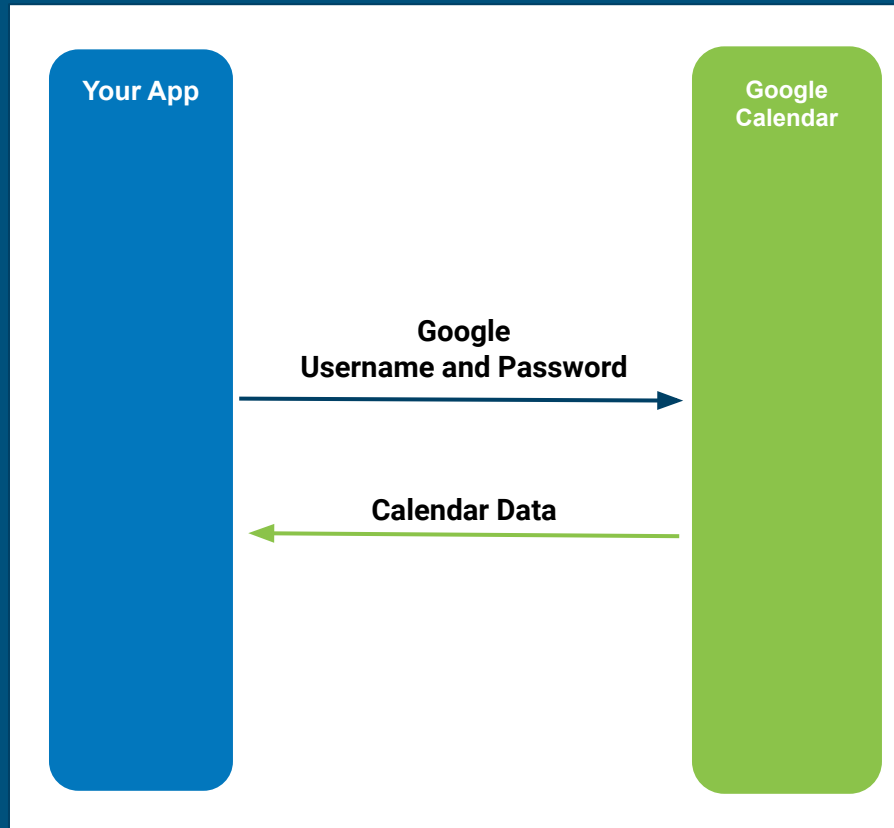
Token created automatically for each user of client app

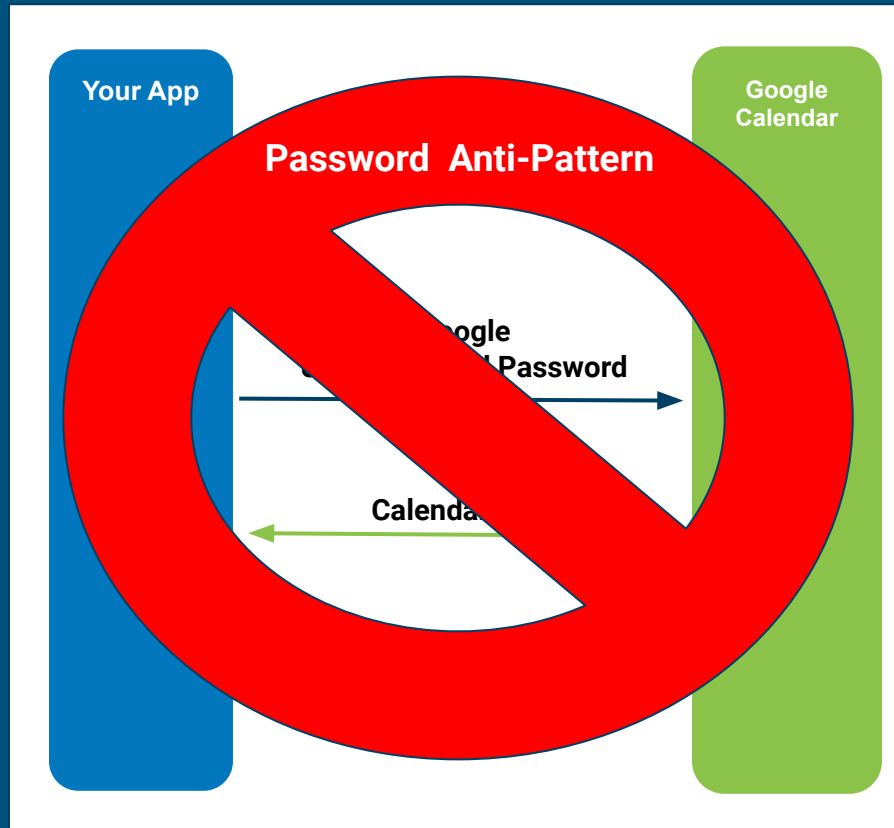
```
Bearer f2507ffa532e873c9360Yb0eu6dr8498fK406844ed75f4Y5b64e2aeb5686e75a
```



A long time ago in a galaxy far,  
far away....







A large, dense crowd of people walking through a subway station. The crowd is diverse in age and appearance. In the background, directional signs for platforms 34 and 35 are visible. The text "No easy way to revoke access from the client App" is overlaid in white on the image.

No easy way to revoke access  
from the client App



Once they're in they're hard to stop





# Access: All or Nothing



User can't remove credentials from  
third-party apps



OAuth

@stmcallister

# OAuth

- ❑ Open standard for authorizing secure access on HTTP service
- ❑ Uses tokens rather than password data to prove identity
- ❑ Provides “secure delegated access” to client applications
- ❑ Limits user’s scope of access





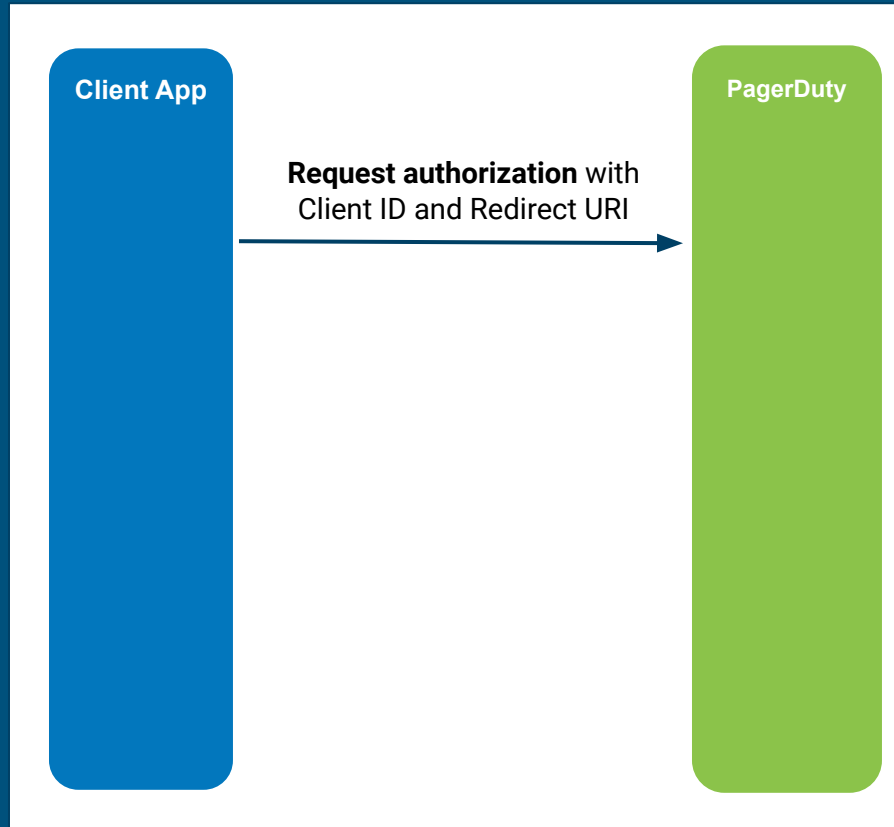
# OAuth with Client Secret

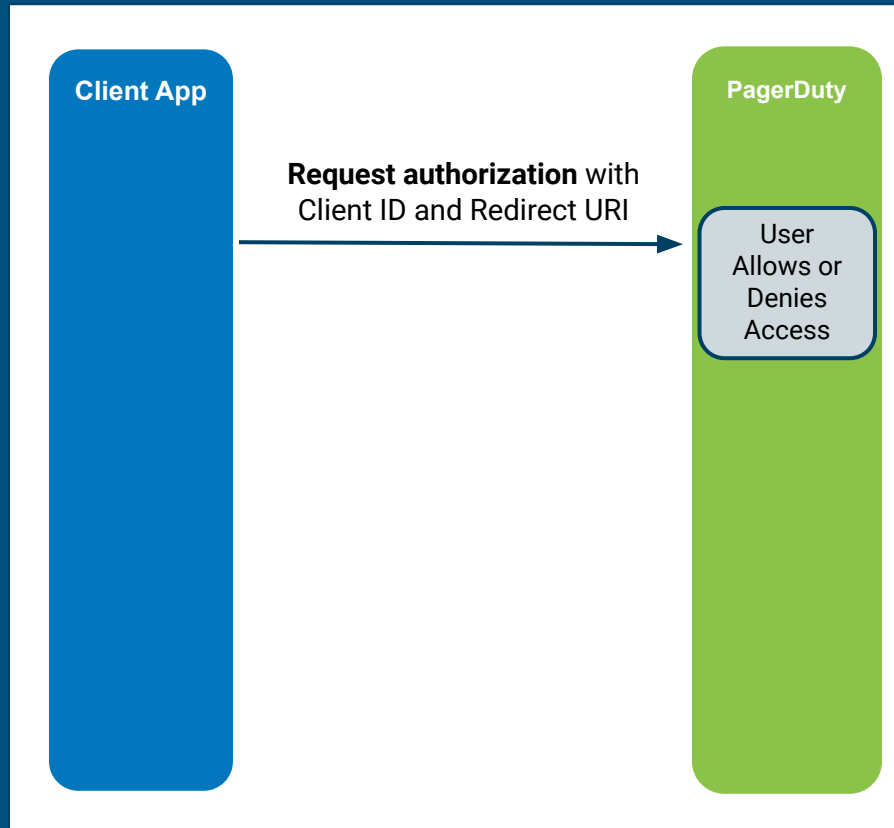
A close-up, high-contrast photograph of a man's face. He has long, light-colored hair and a full beard. His eyes are a striking blue, and he is looking directly at the camera with a serious expression. The lighting is dramatic, with deep shadows and bright highlights, creating a moody atmosphere. The text "Keep it Secret. Keep it safe." is overlaid in the center of the image.

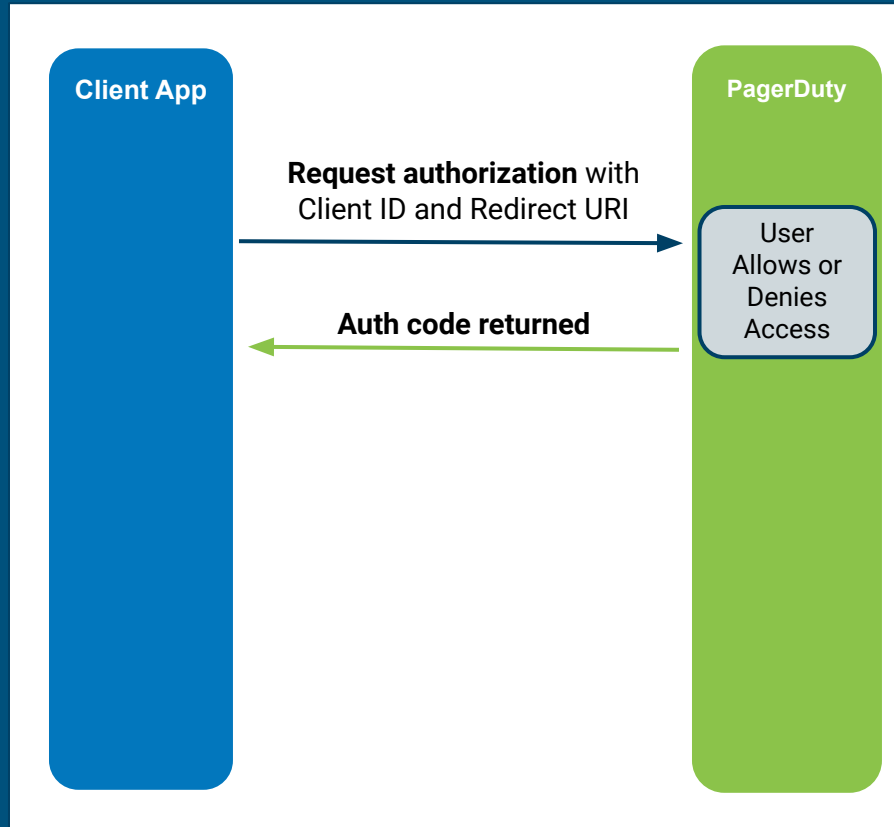
Keep it Secret. Keep it safe.

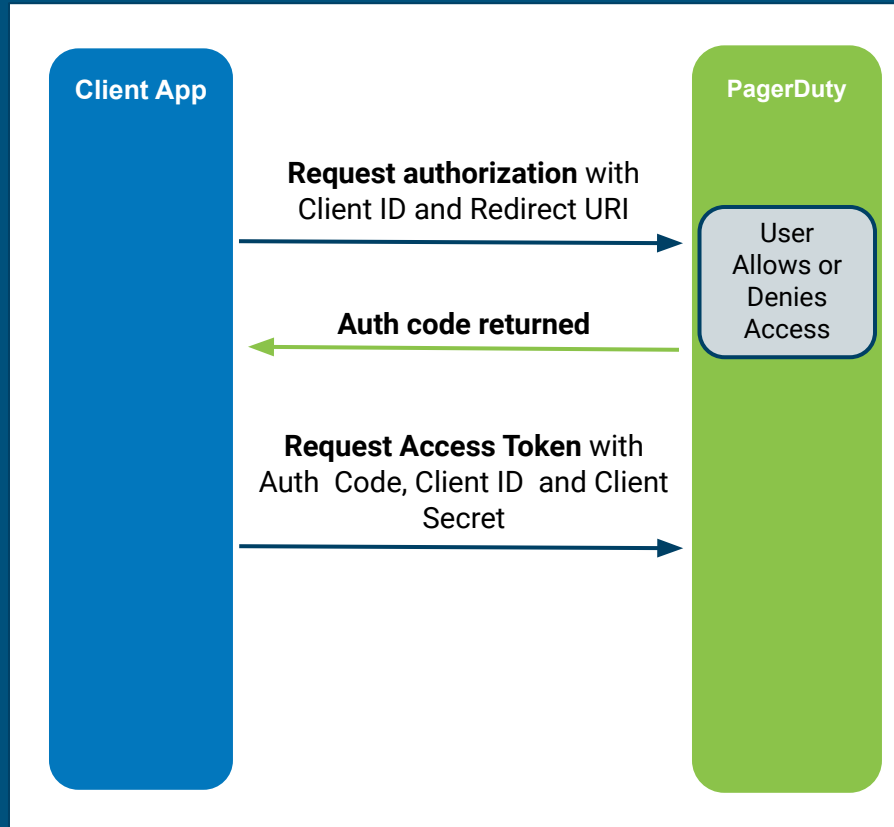
@stmcallister

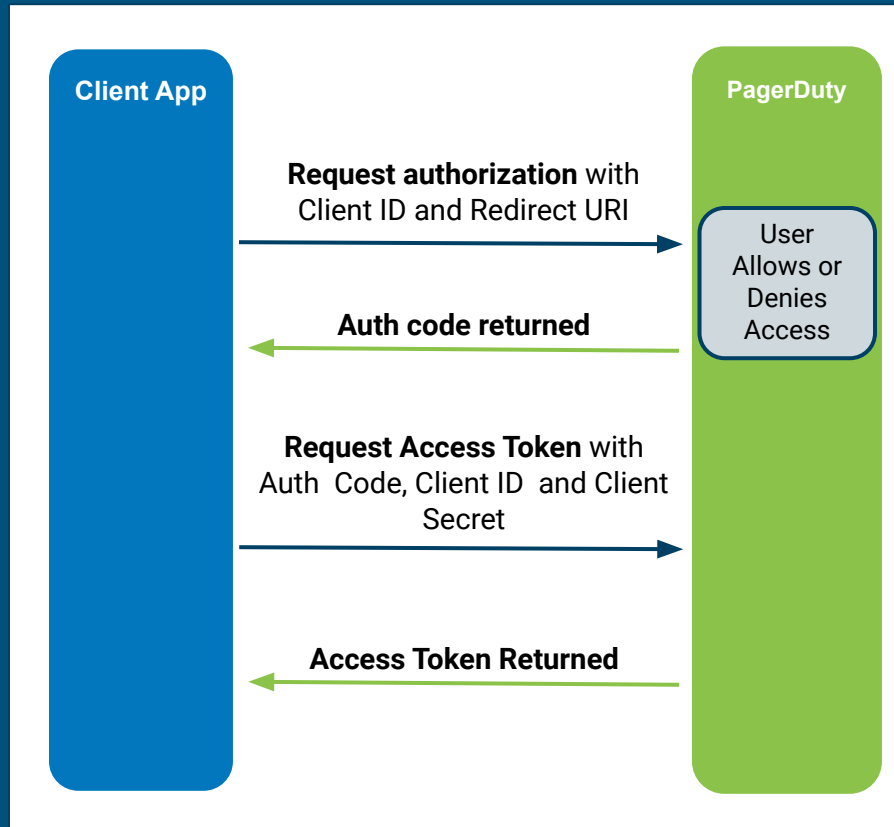














# OAuth with Proof Key for Code Exchange (PKCE)



# PKCE Terms

- ❑ Code\_verifier
  - ❑ Random 128byte, base64 urlEncoded value
- ❑ Code\_challenge
  - ❑ Hashed, base64 urlEncoded (no padding) value of Code\_verifier
- ❑ Challenge\_method
  - ❑ Method of hash used

Client App

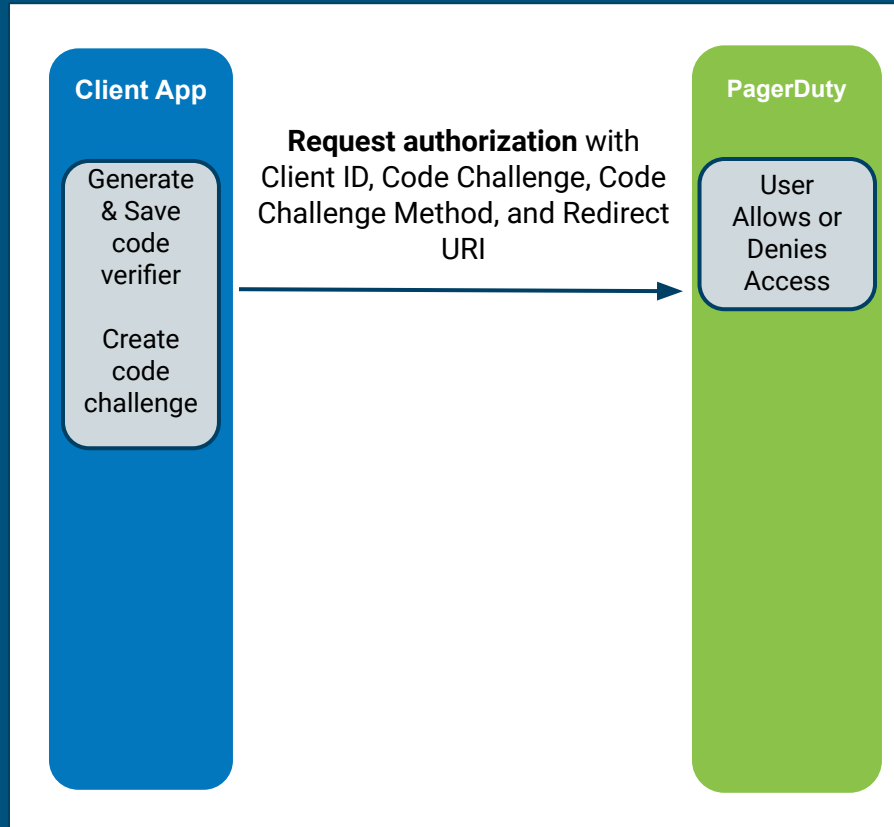
PagerDuty

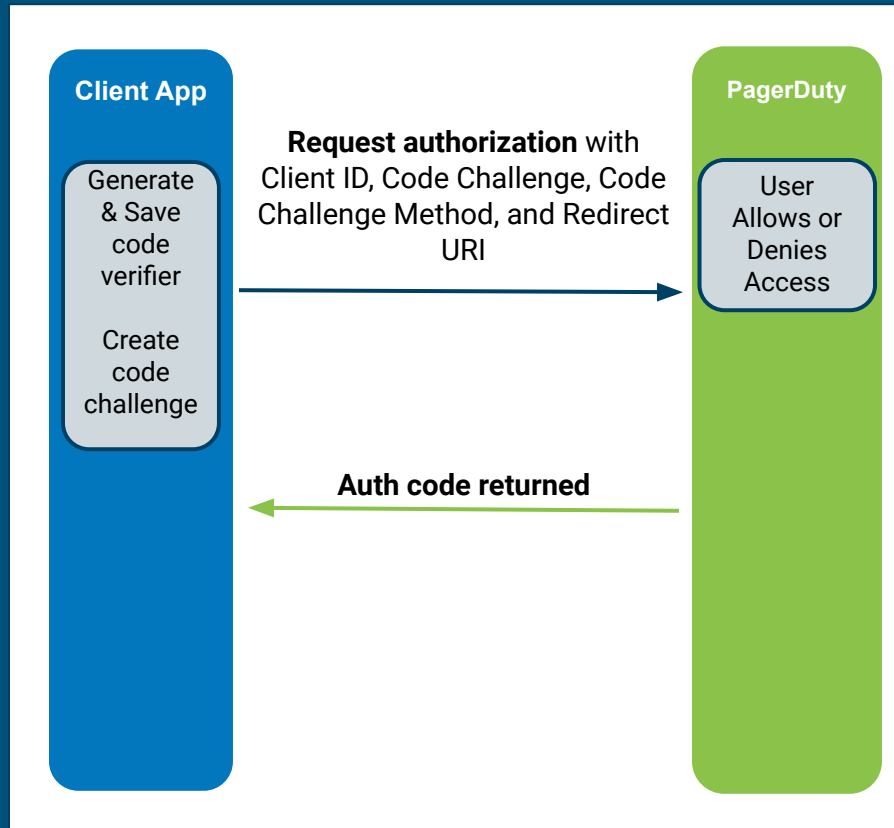
## Client App

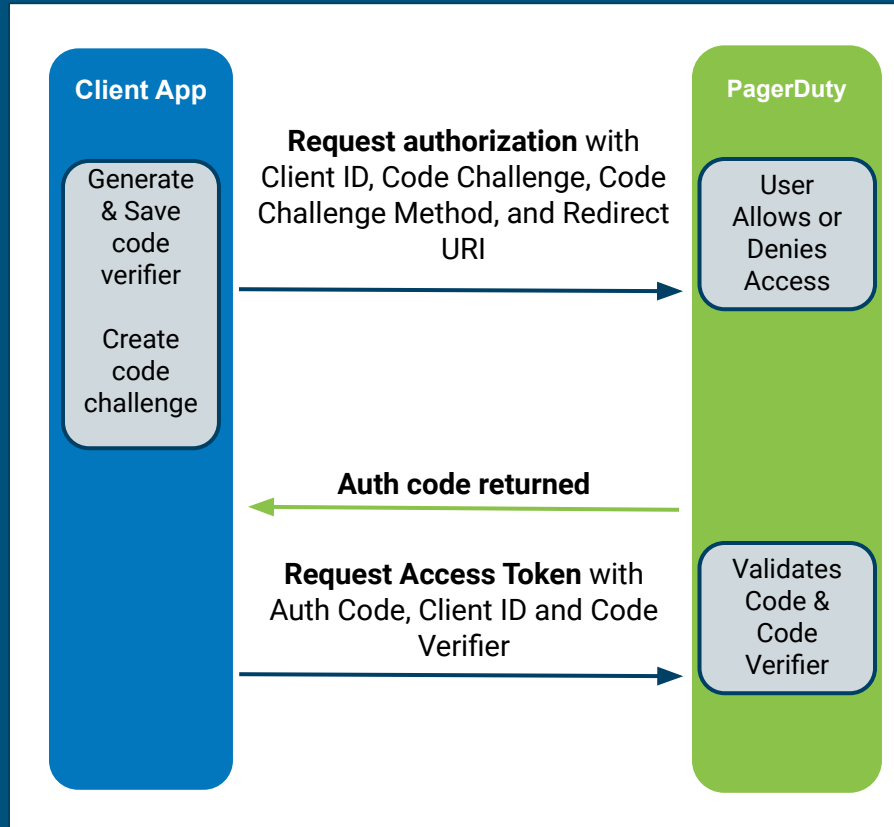
Generate  
& Save  
code  
verifier

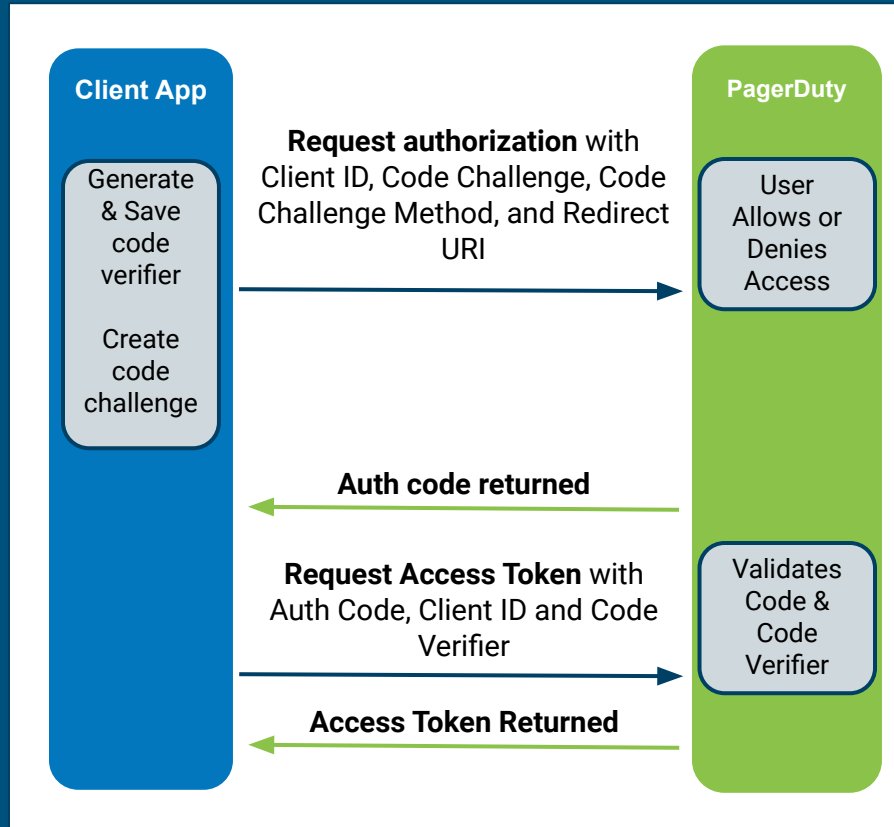
Create  
code  
challenge

## PagerDuty











# Automation

@stmcallister



# How to get updates?

Polling vs Webhooks

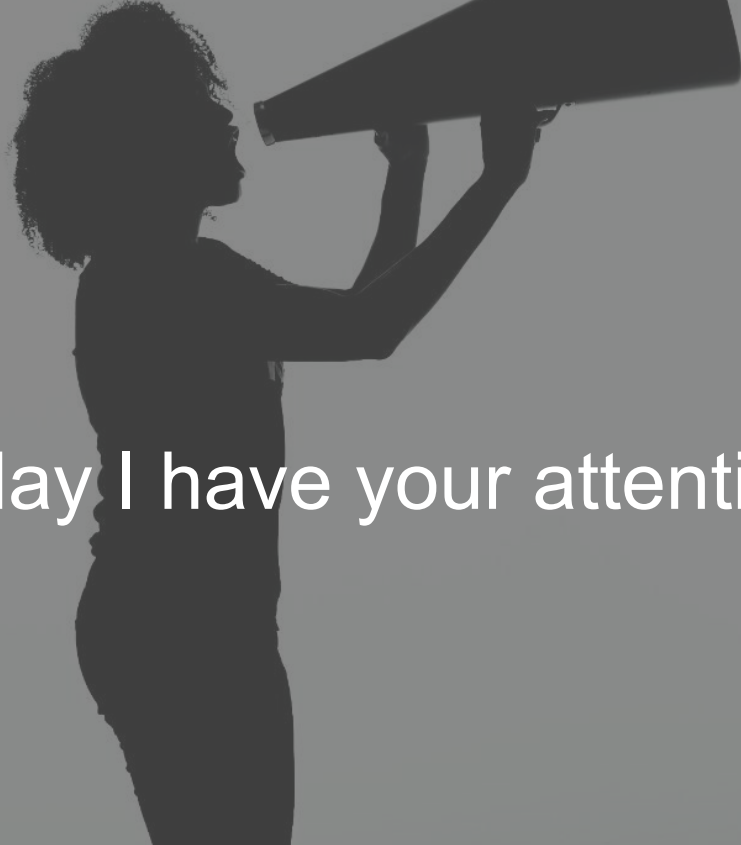
# Polling

A woman with long, wavy red hair and bright blue eyes is looking directly at the camera with a serious, intense expression. Her hands are raised to her temples, with her fingers spread. She has red nail polish on her fingers and a black and white striped pattern on her thumbnails. She is wearing a silver bracelet with white beads on her left wrist. The background is a plain, light gray.

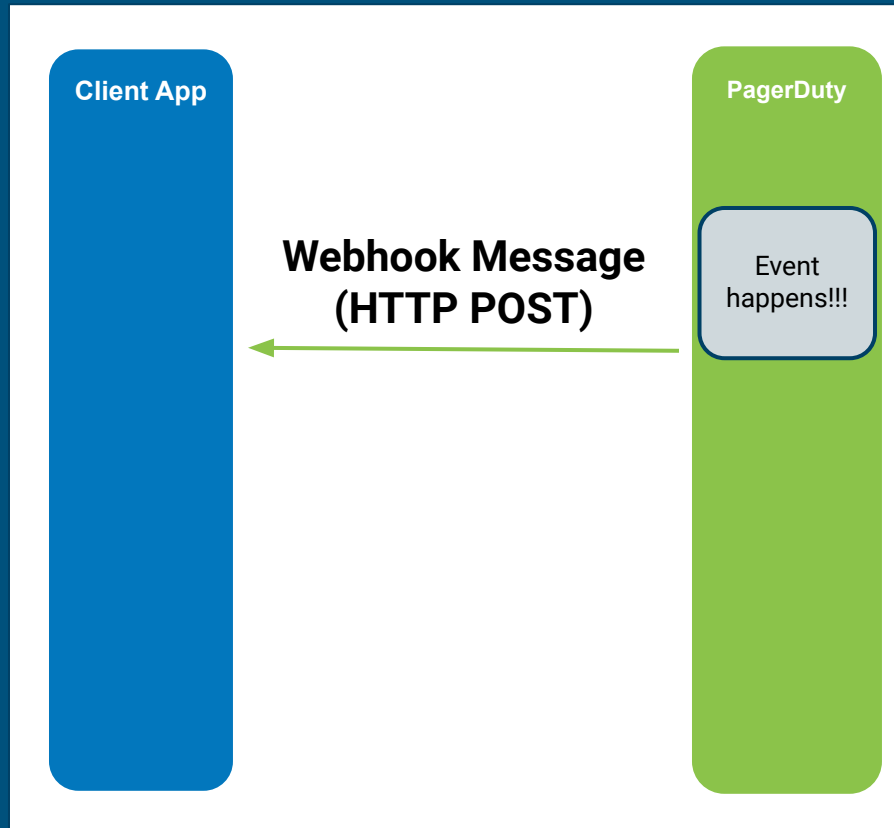
Are you done yet?

@stmcallister

# Webhooks



May I have your attention, please!



# Webhook Payloads

Thin vs..Not so thin?

**OVERSIZE LOAD**



# Thin Payload

```
{
  "nonce": "4b2ed20d-6f00-4b0c-8fac-082182aa9aac",
  "timestamp": "2015-10-27T17:04:23.795+0000",
  "webhookId": 4503604829677444,
  "scope": "sheet",
  "scopeObjectId": 4509506114742148,
  "events": [
    {
      "objectType": "sheet",
      "eventType": "updated",
      "id": 4509506114742148,
      "userId": 9007194052434043,
      "timestamp": "2015-10-27T17:03:15.000+0000"
    },
    {
```

# “Heavy” Payload

```
{
  "event": {
    "id": "5ac64822-4adc-4fda-ade0-410becf0de4f",
    "event_type": "incident.priority_updated",
    "resource_type": "incident",
    "occurred_at": "2020-10-02T18:45:22.169Z",
    "agent": {
      "html_url": "https://acme.pagerduty.com/users/PLH1HKV",
      "id": "PLH1HKV",
      "self": "https://api.pagerduty.com/users/PLH1HKV",
      "summary": "Tenex Engineer",
      "type": "user_reference"
    },
  },
  "client": {
    "name": "PagerDuty"
  },
  "data": {
    "id": "PGR0VU2",
    "type": "incident",
    "self": "https://api.pagerduty.com/incidents/PGR0VU2",
    "html_url": "https://acme.pagerduty.com/incidents/PGR0VU2",
    "number": 2,
    "status": "triggered",
    "title": "A little bump in the road"
```

# Rate Limiting: Call Limit vs Rate Limit

## Call Limit

number of times API invoked in a certain time period usually as business choice

## Rate Limit

imposed for reasons of fairness so one customer doesn't overwhelm infrastructure and affect other customers



# Rate Limiting: Rate Limit Response

The response to the API call will say

429 – Request Limit Exceeded

A person with short brown hair, seen from the back, is looking at a wall covered in various sticky notes, diagrams, and sketches. The person is wearing a light-colored sweater with dark horizontal stripes. The wall behind them is densely packed with papers, some containing flowcharts, diagrams, and handwritten notes. The overall scene suggests a creative or collaborative work environment.

# Developer Experience

@stmcallister

# Download Postman

Download the app to quickly get started using the Postman API Platform. Or, if you prefer a browser experience, you can try the new web version of Postman.

## The Postman app

The ever-improving Postman app (a new release every two weeks) gives you a full-featured Postman experience.

[Download the App](#)

By downloading and using Postman, I agree to the [Privacy Policy](#) and [Terms](#).

Version 8.11.1 | [Release Notes](#) | [Product Roadmap](#)

Not your OS? Download for Windows (x32 / x64) or Linux (x64)

## Postman on the web

The screenshot shows the Postman web interface with a REST client for the Twitter API. The URL is `https://api.twitter.com/2/tweets/id` and the method is GET. The interface includes tabs for Params, Authorization, Headers, Body, Pre-request Scripts, Tests, Settings, and Cookies. A table of query parameters is visible, with the 'id' parameter checked and set to '1403216129661628420'.

Key	Value	description
<input type="checkbox"/>	tweet.fields	attachments,author_id,context_annotations,conversatio...
<input type="checkbox"/>	expansions	Comma-separated list of fields to expand. Expansions e...
<input type="checkbox"/>	media.fields	duration_ms,height_media_key_non_public_metrics,organ...
<input type="checkbox"/>	poll.fields	Comma-separated list of fields for the poll object. Expl...
<input type="checkbox"/>	place.fields	Comma-separated list of fields for the place object. Exp...
<input type="checkbox"/>	user.fields	Comma-separated list of fields for the user object. Expl...

Key	Value	description
<input checked="" type="checkbox"/>	id	Required. Enter a single Tweet ID.



# Scott McAllister

Speaker, Writer, Coder

PagerDuty

 [stmcallister.github.io](https://stmcallister.github.io)

 [@stmcallister](https://twitter.com/stmcallister)

