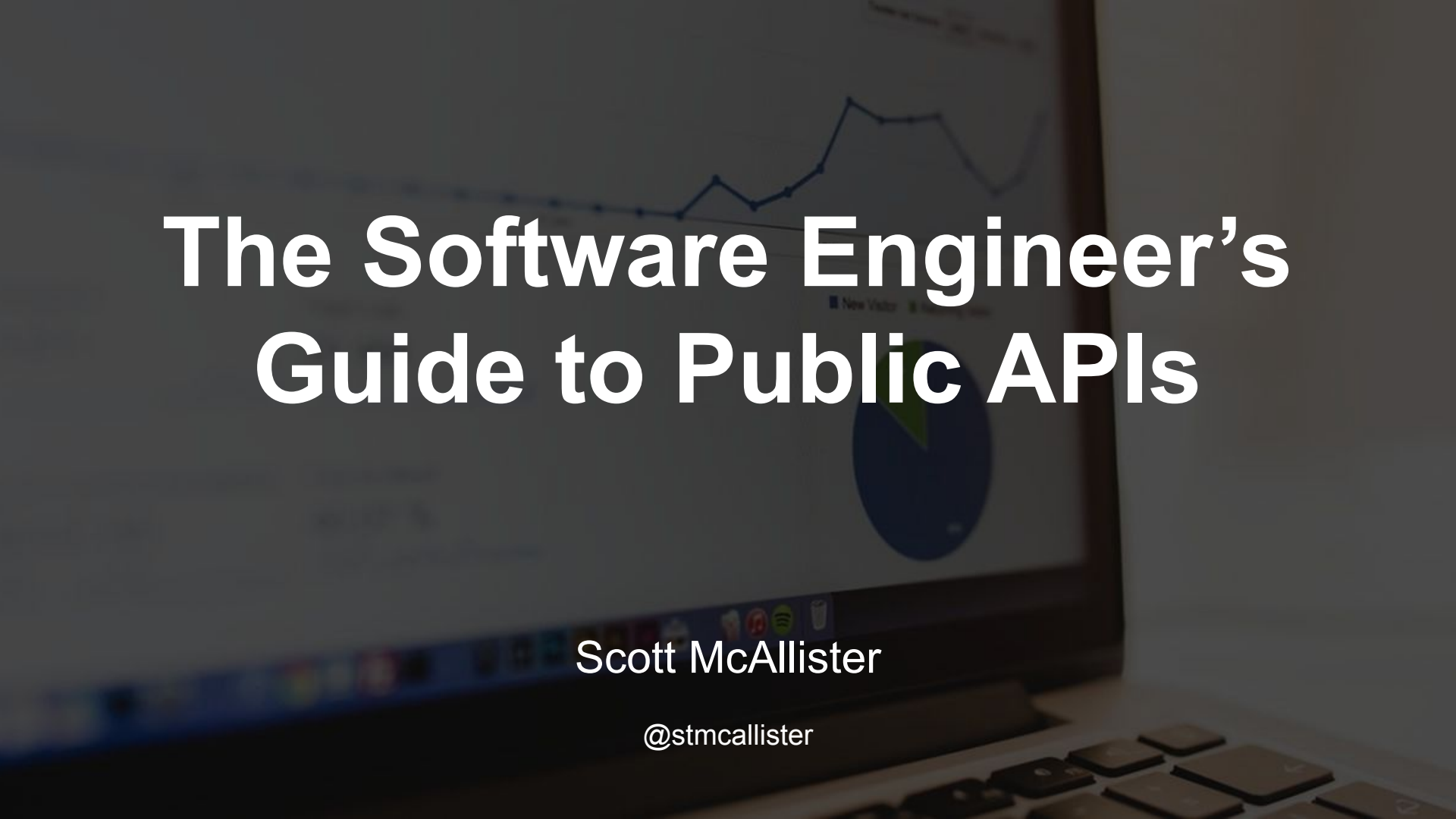


The Software Engineer's Guide to Public APIs

Scott McAllister

@stmcallister

Titanium Sponsors

okta

Headspring

Platinum Sponsors

PAIGE TECHNOLOGIES
INTELLIGENT PAIRING. PERPETUAL SUCCESS.

EVENT STORE.

Homebase

Dimensional Innovations

WellSky

DevExpress®

Progress® Telerik®

Algorand

AxonIQ

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

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

AMERICAN EXPRESS PayPal

Get around

DELTA priceline.com

Do work

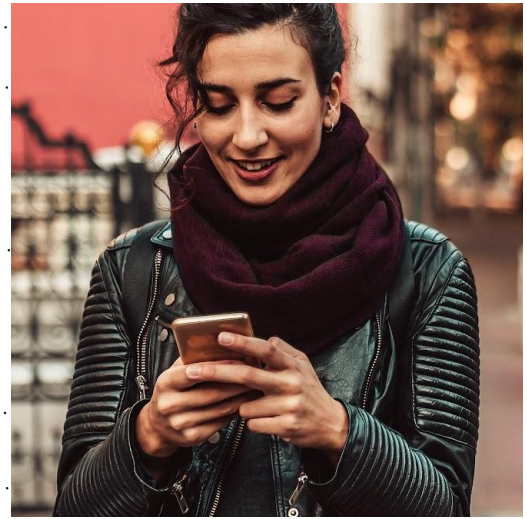
salesforce box

Buy anything

COSTCO WHOLESALE Walmart

Stay healthy

fitbit



Shop online

AMERICAN EAGLE GAP

Be entertained

NETFLIX The New York Times

Order food

EAT24 Blue Apron

Be connected

Linked in

@stmcallister

What is an API?

Messenger that sends and receives requests for an application

API Standards

HTTP

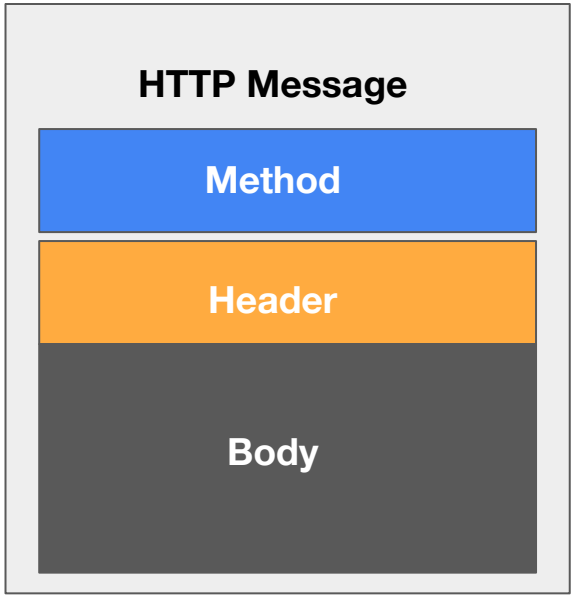
POST → **Create** data

GET → **Read** data

PUT → **Update** data

DELETE → **Delete** data

HTTP Messages



The action being taken. POST, GET, PUT, DELETE

Information about the data in the message

Data being sent

Authorization Header

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

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

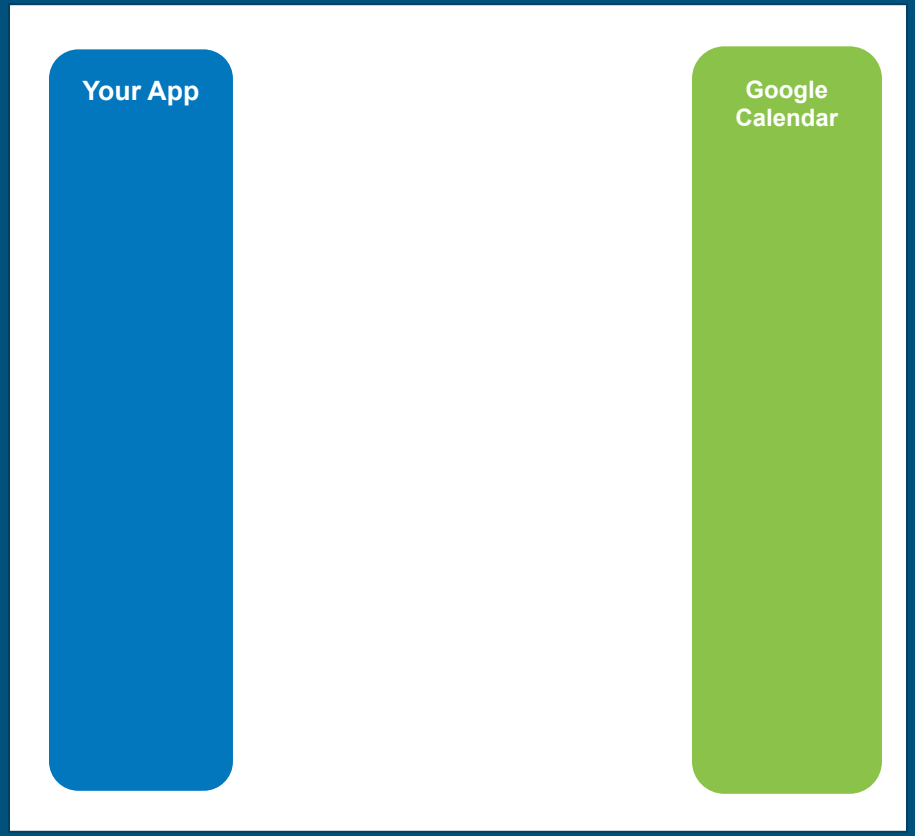
Authentication

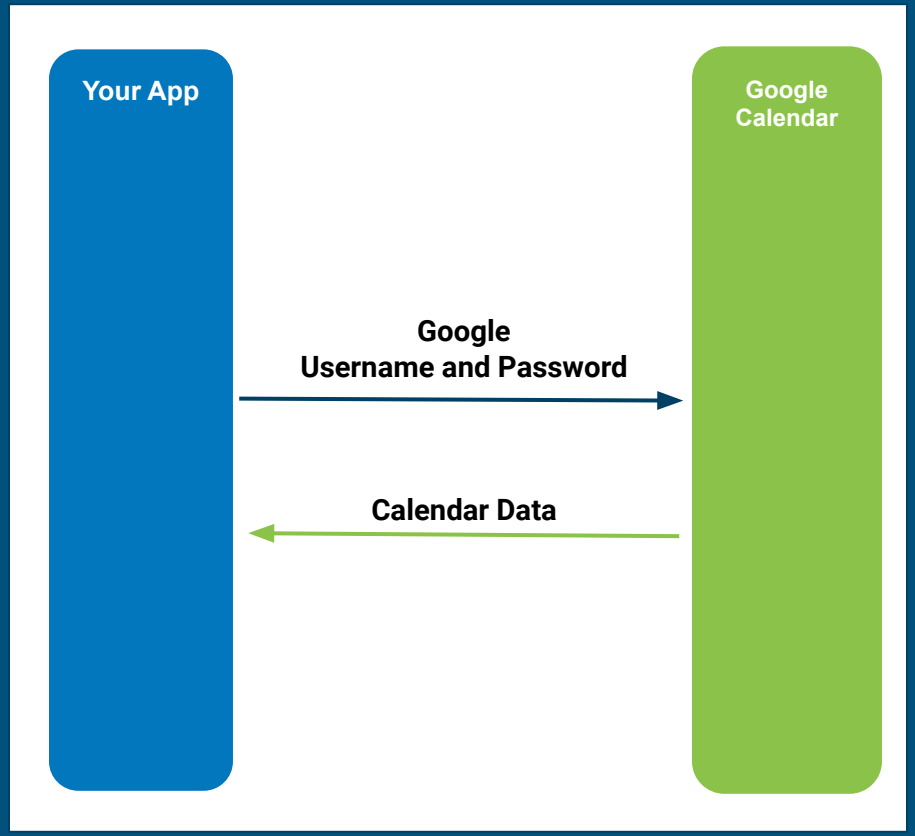
OAuth

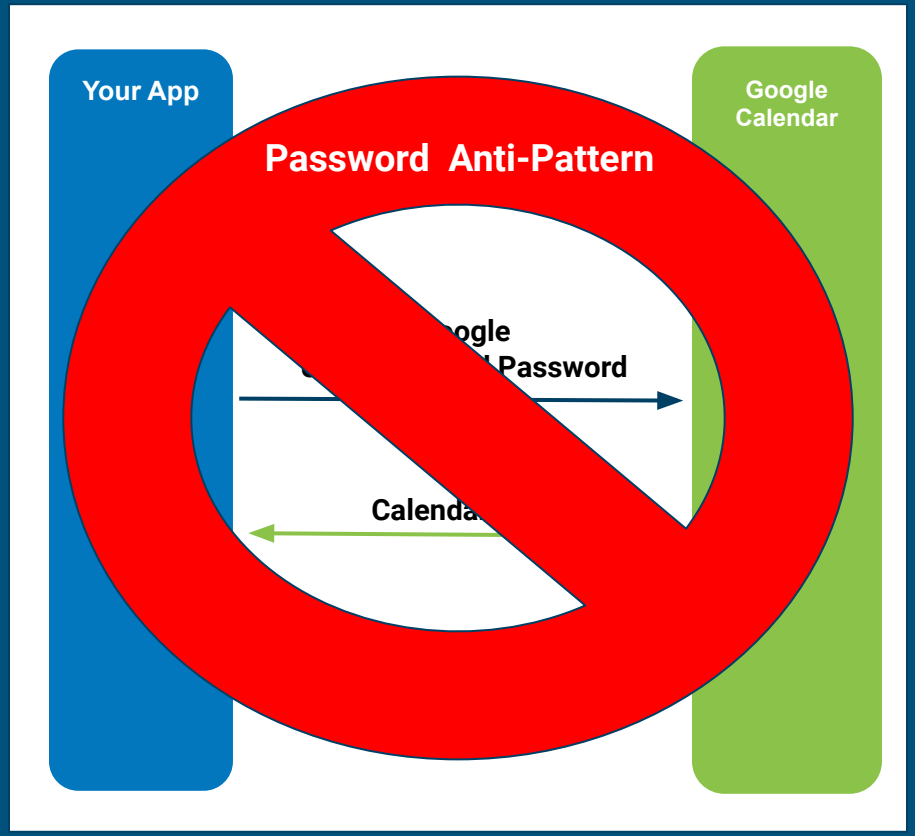
Token created automatically for each user of client app

```
Bearer f2507ffa532e873c9360Yb0eu6dr8498fK406844ed75f4Y5b64e2aeb5686e75a
```

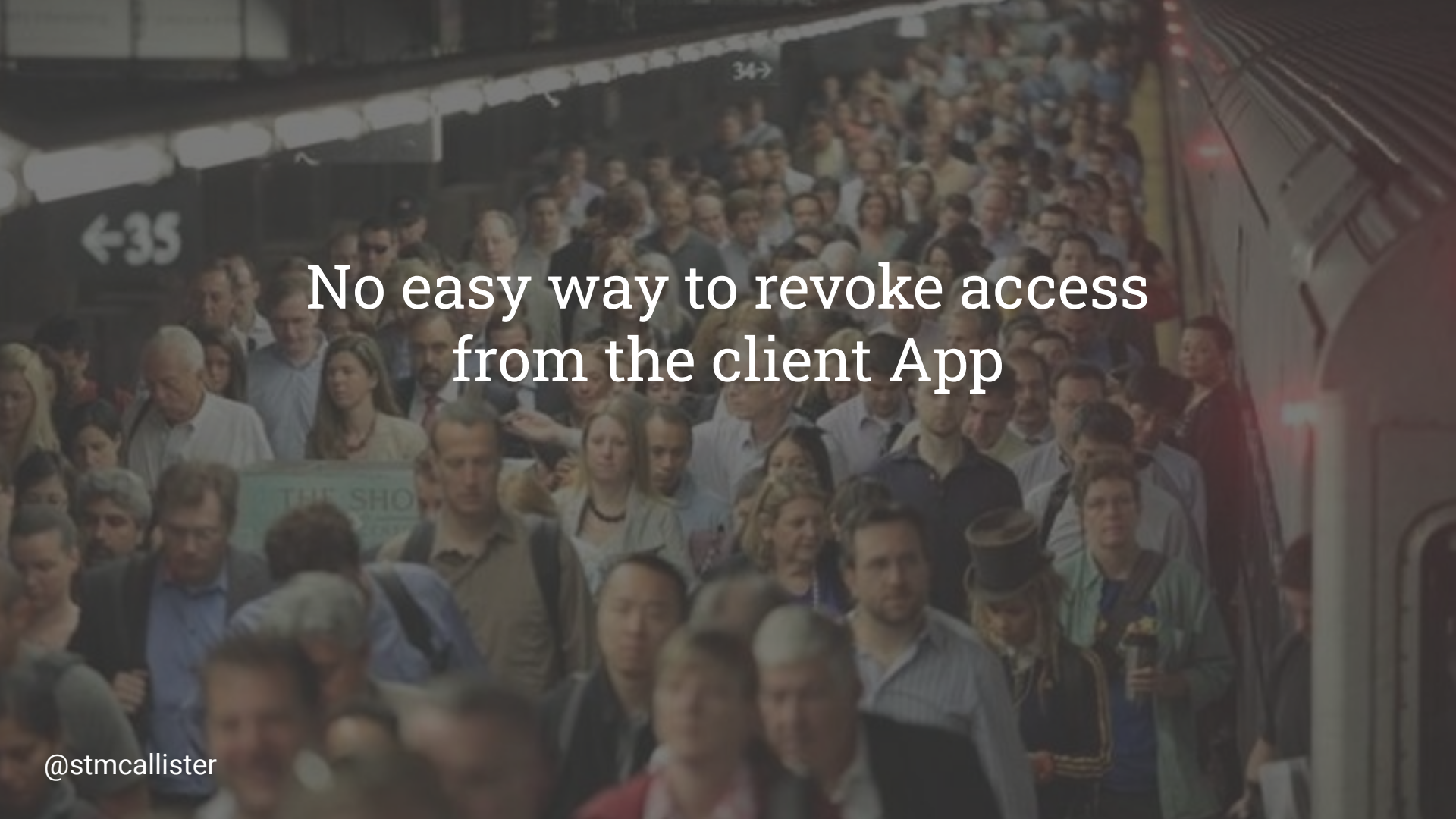
A long time ago in a galaxy far, far away....


Your App
Google Calendar


Your App
Google Calendar
Google
Username and Password
Calendar Data



@stmcallister

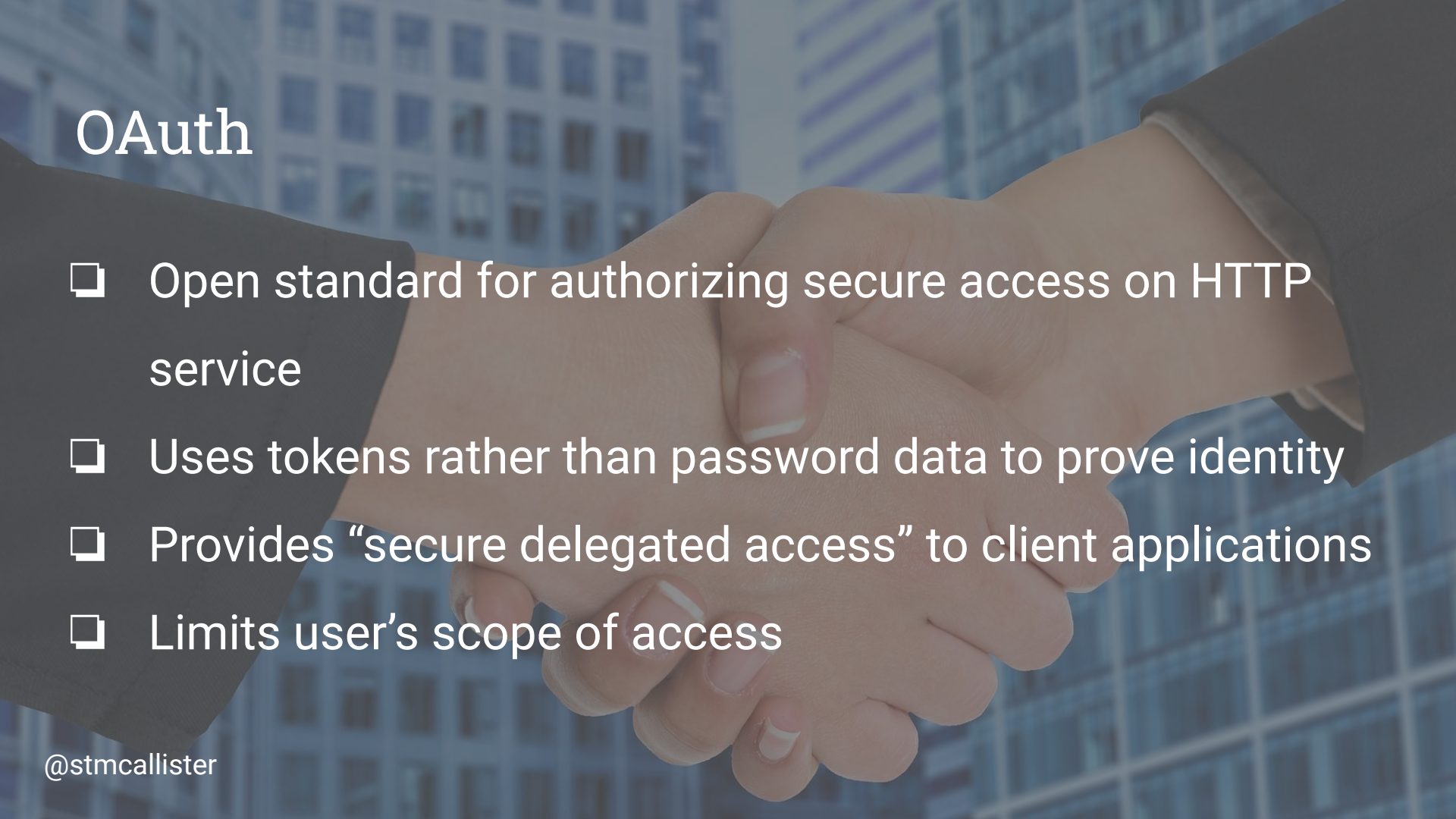

No easy way to revoke access
from the client App
@stmcallister

@stmcallister


Access: All or Nothing


User can’t remove credentials from third-party apps
@stmcallister


OAuth
@stmcallister

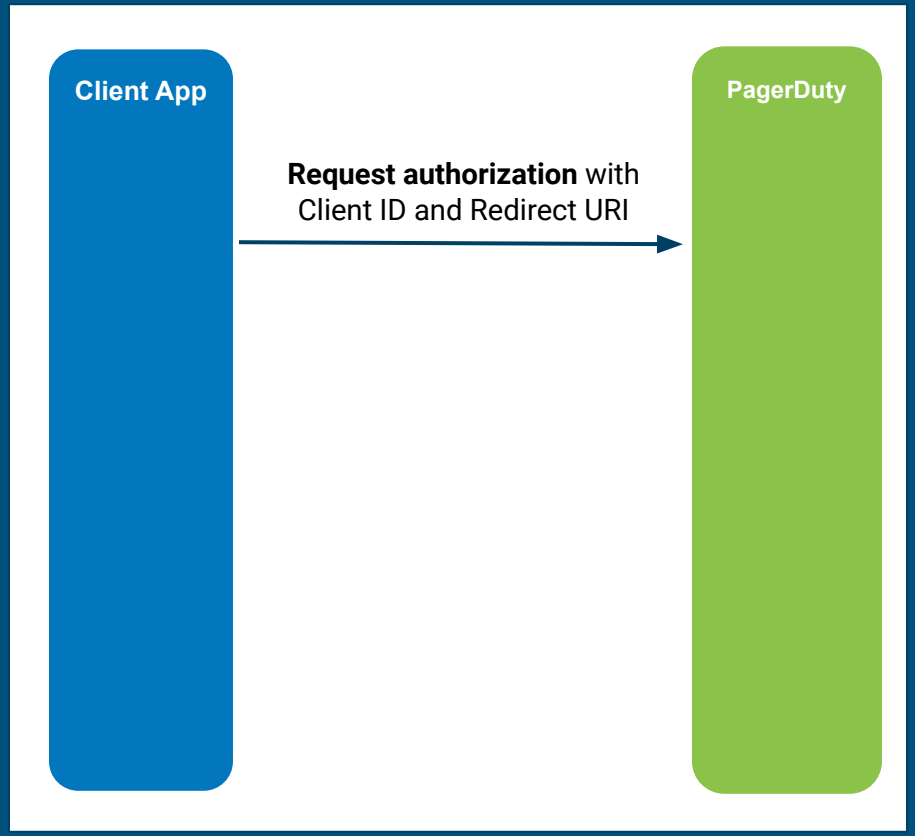


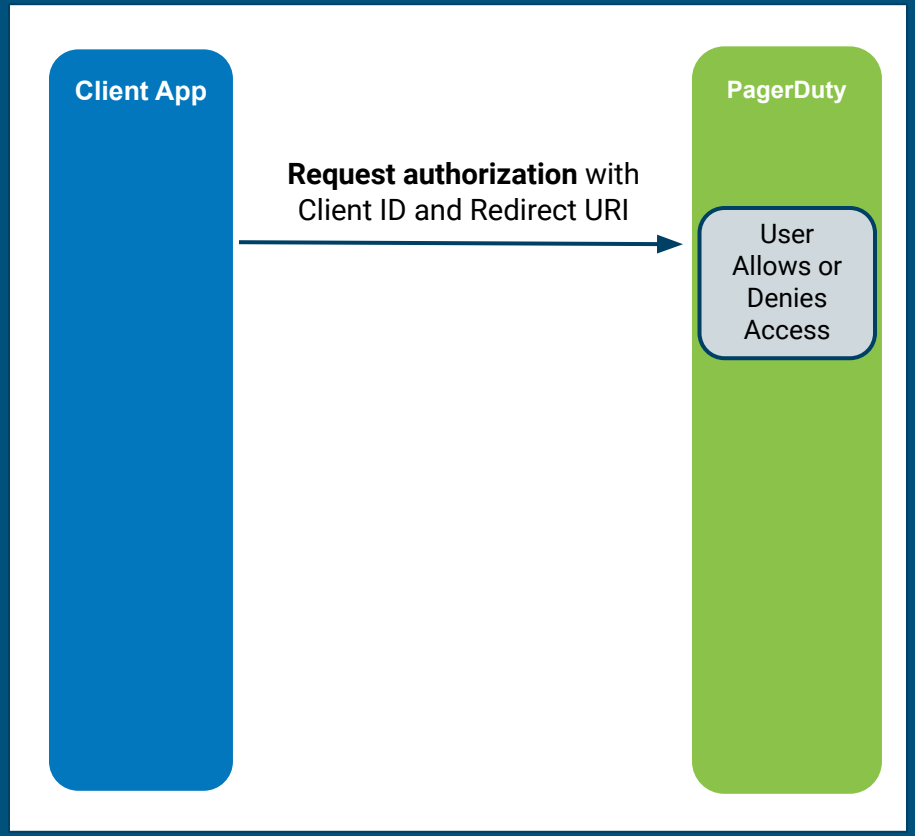
OAuth

- 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

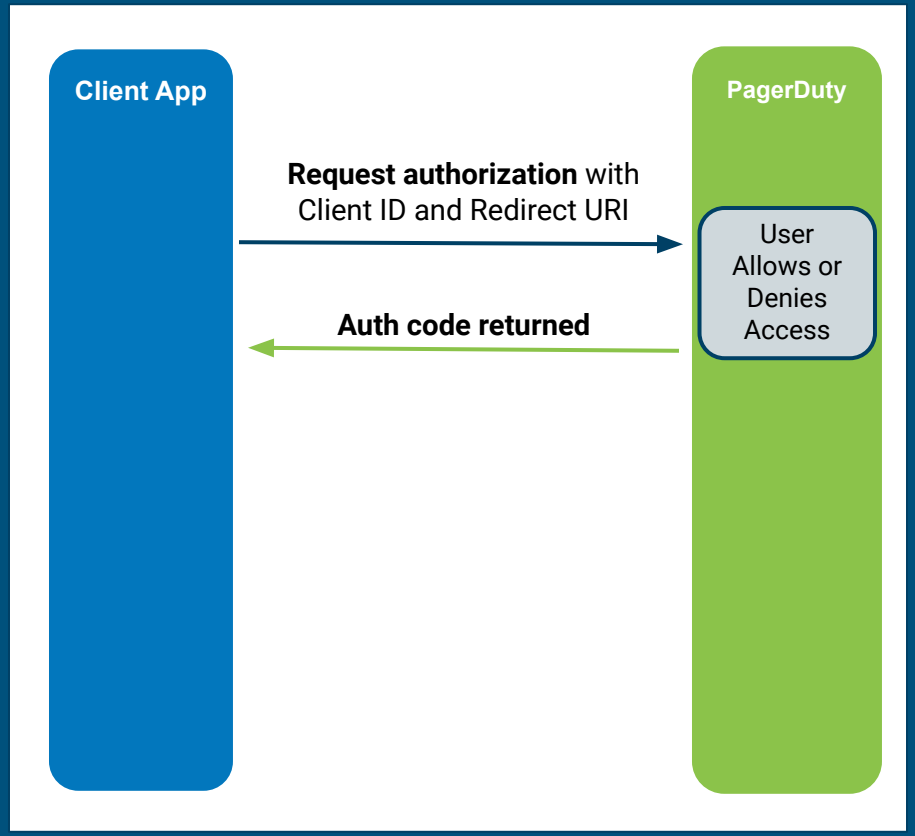

OAuth with Client Secret
@stmcallister


Keep it Secret. Keep it safe.
@stmcallister

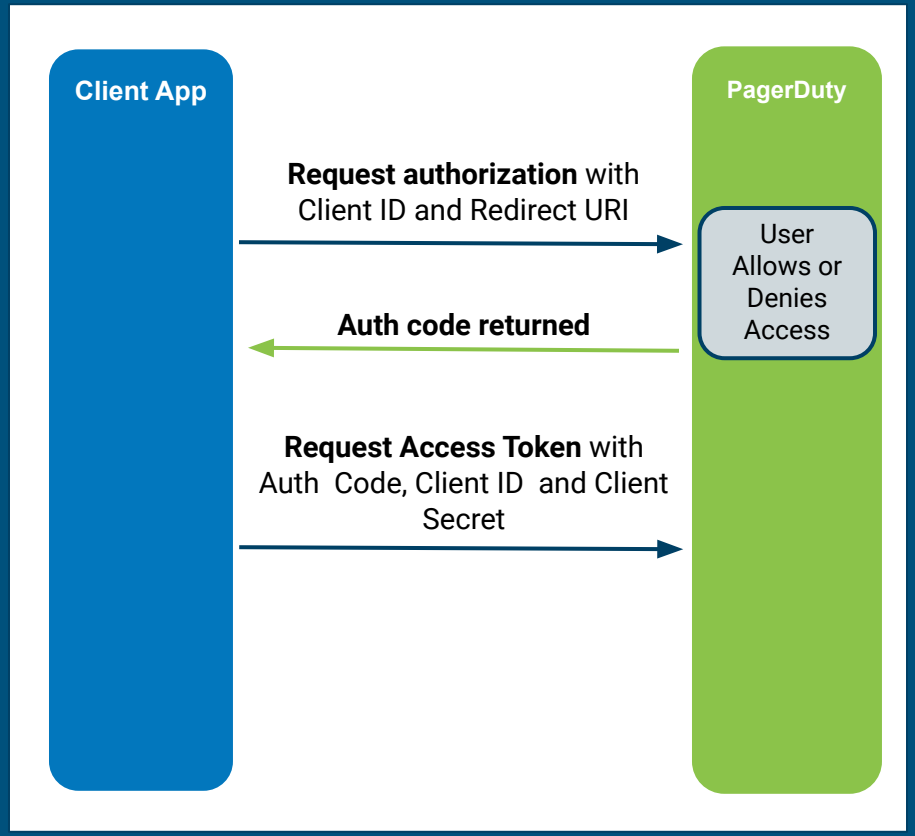

Client App
PagerDuty
Request authorization with
Client ID and Redirect URI



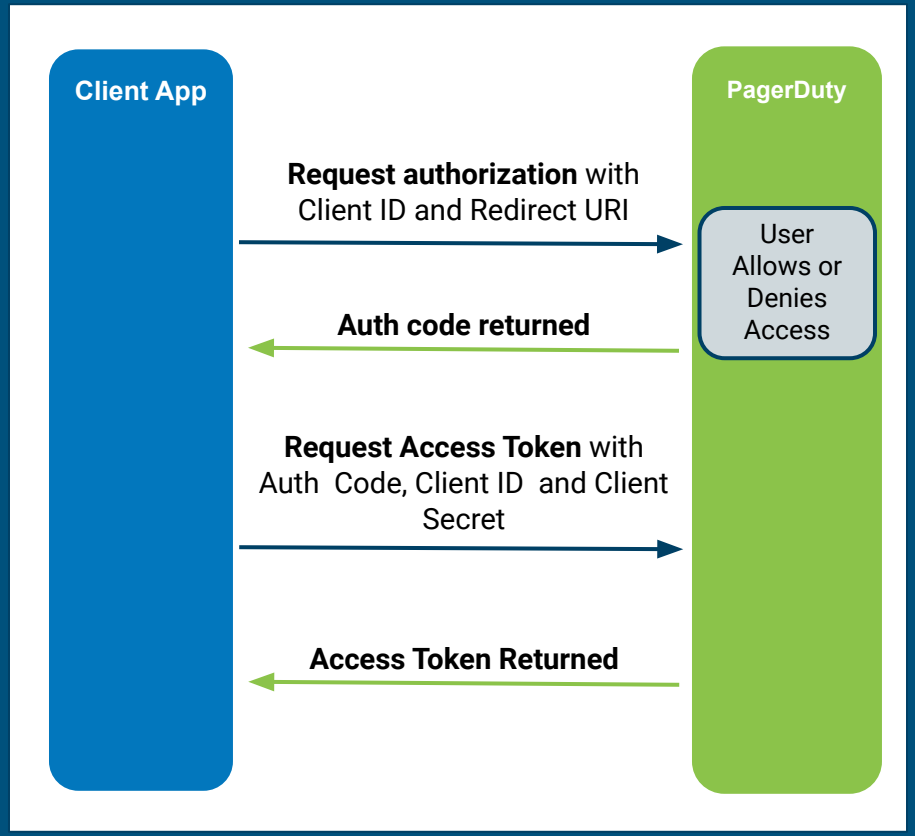
@stmcallister



@stmcallister



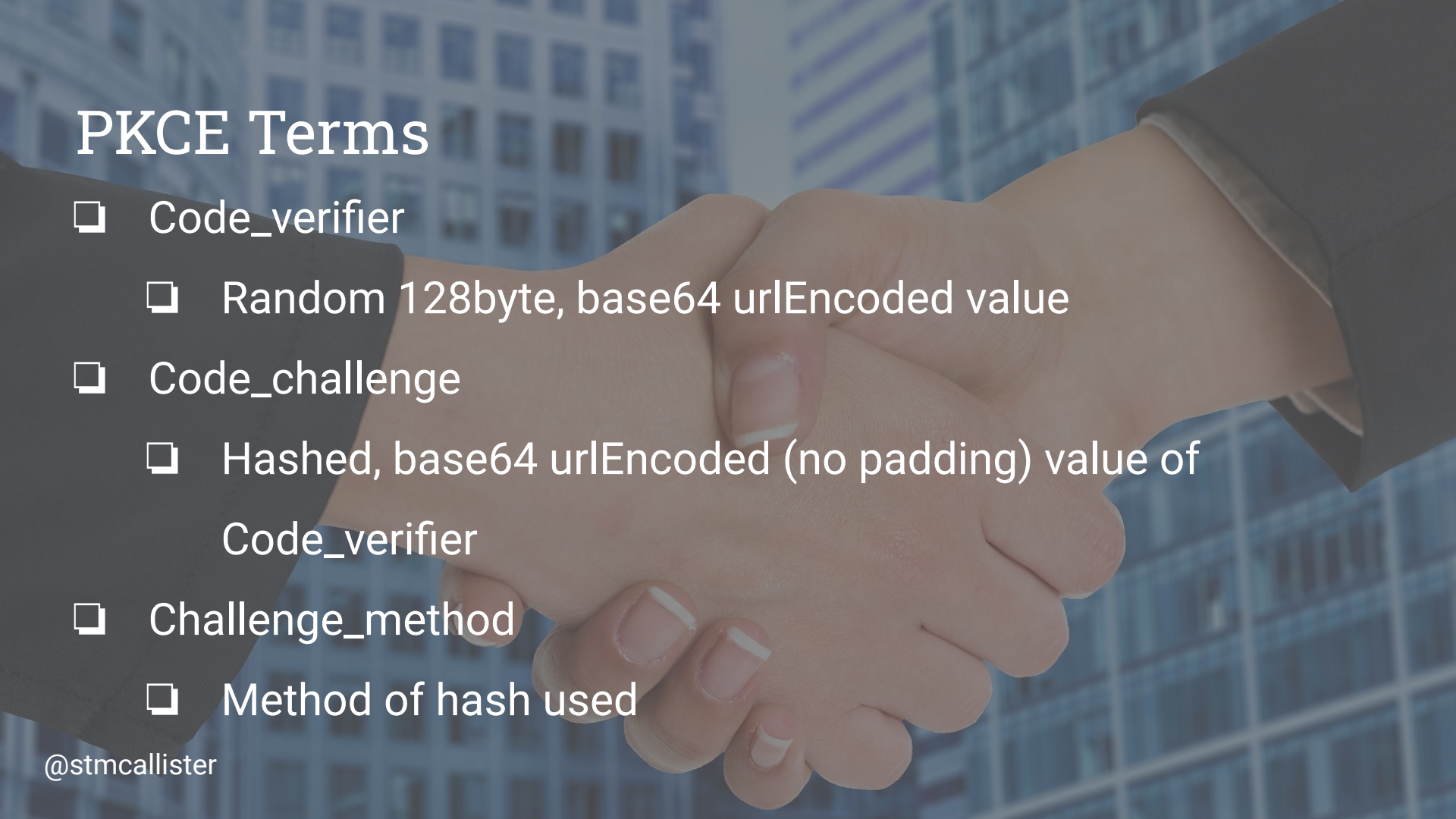
@stmcallister



@stmcallister

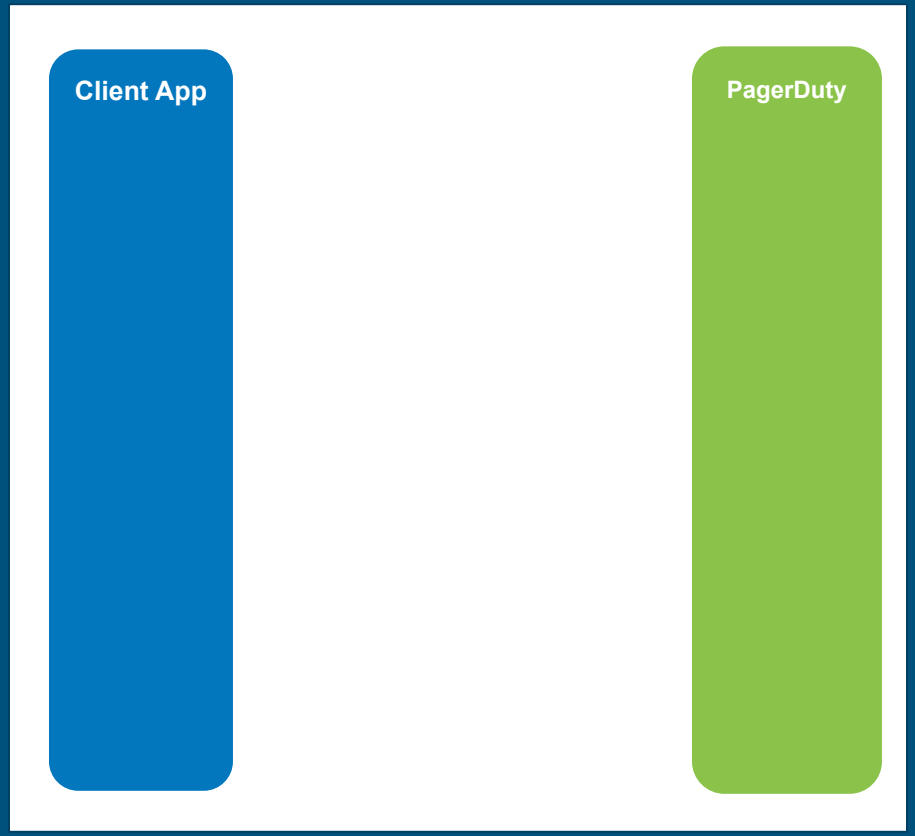
OAuth with Proof Key for Code Exchange (PKCE)

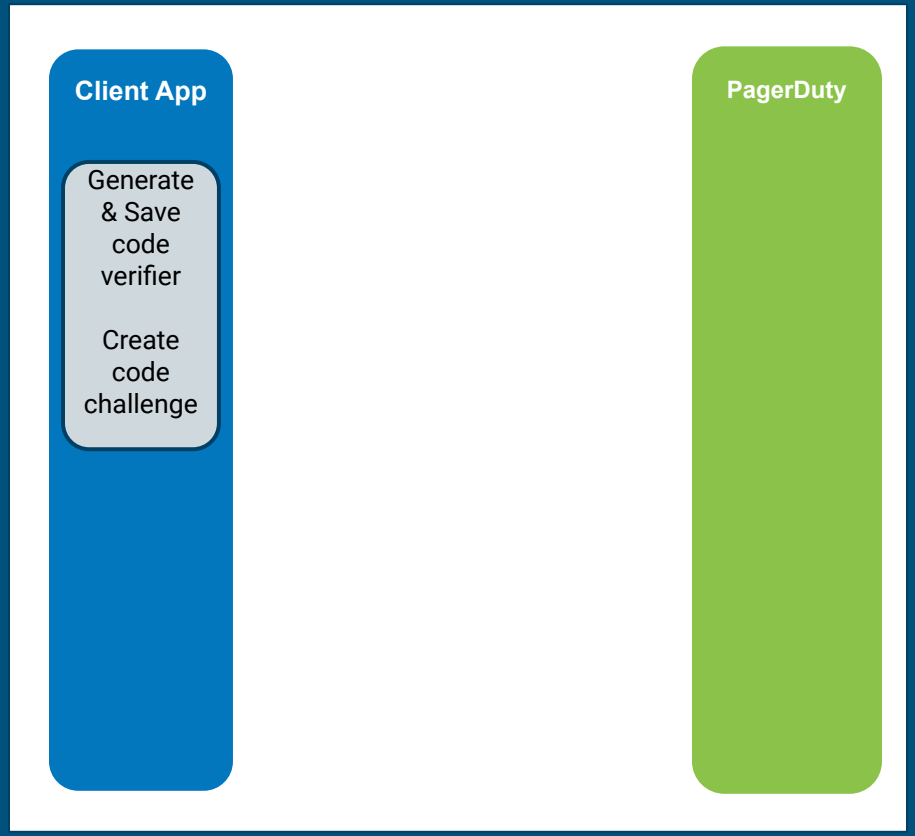
@stmcallister

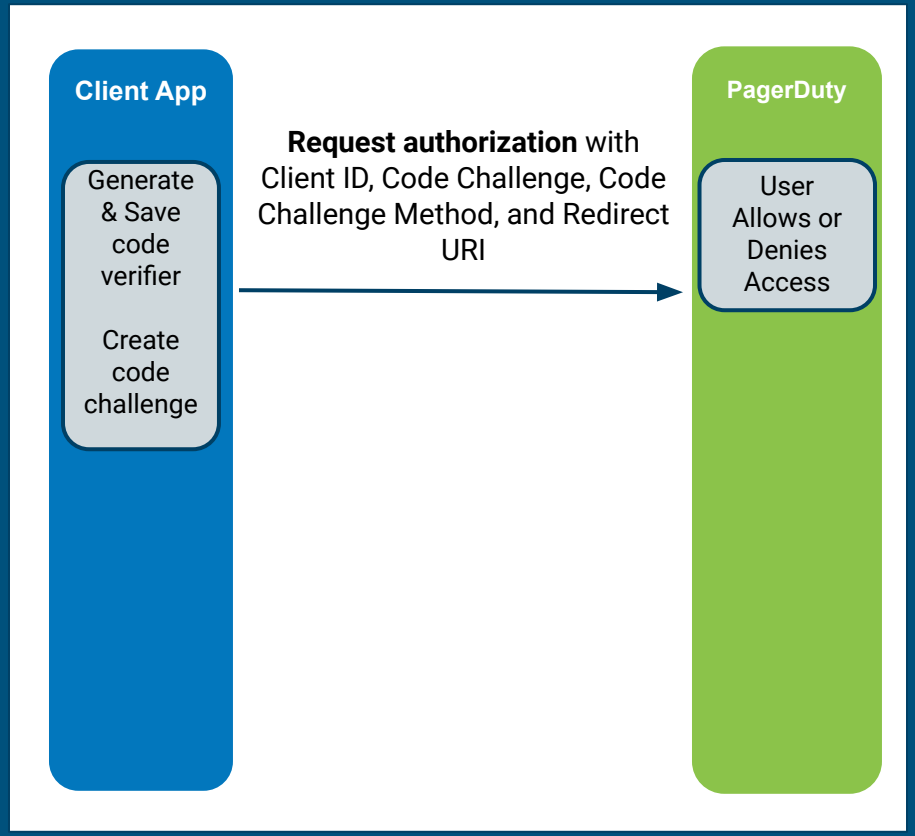


PKCE Terms

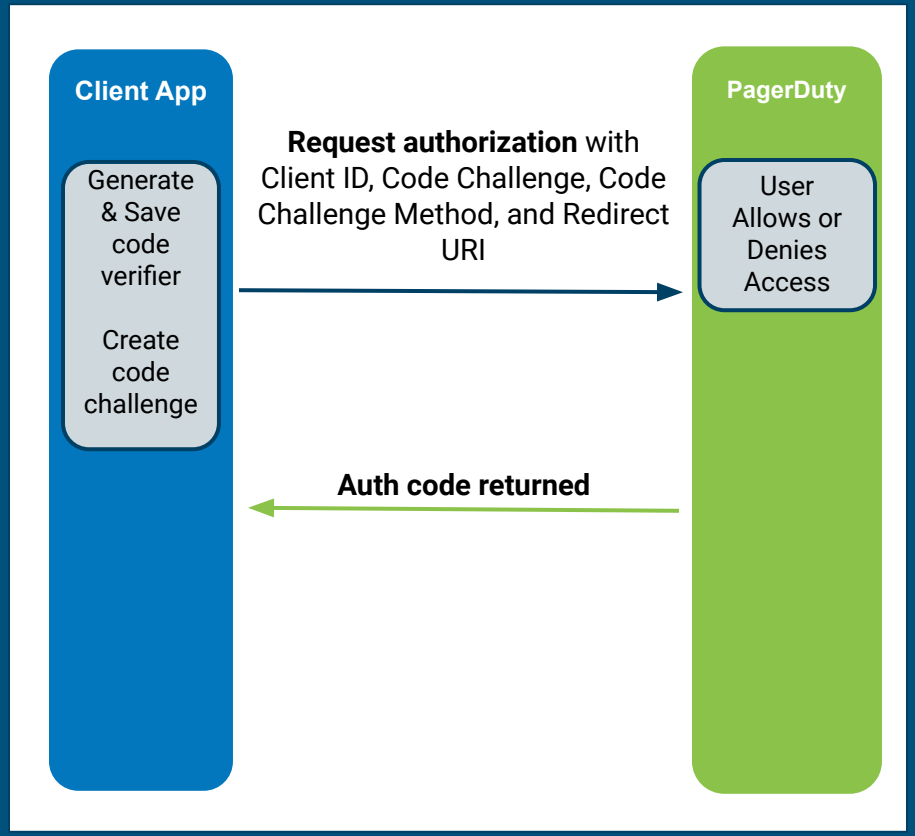
- Code_verifier
  - Random 128byte, base64 urlEncoded value
- Code_challenge
  - Hashed, base64 urlEncoded (no padding) value of Code_verifier
- Challenge_method
  - Method of hash used


Client App
PagerDuty

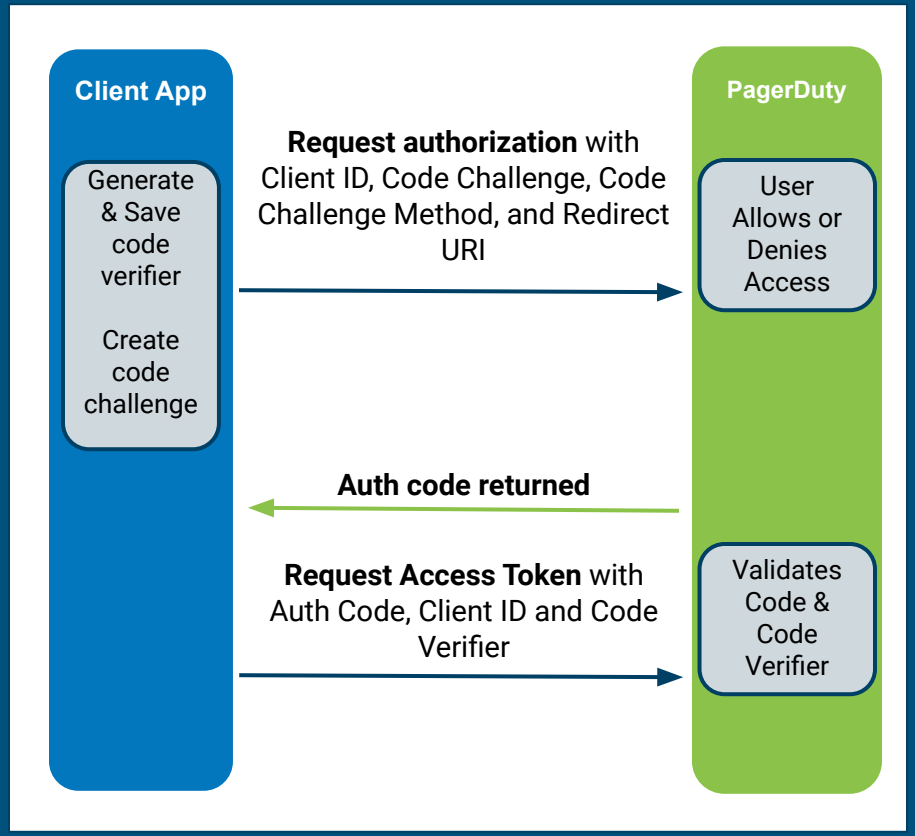

Client App
Generate & Save code verifier
Create code challenge
PagerDuty



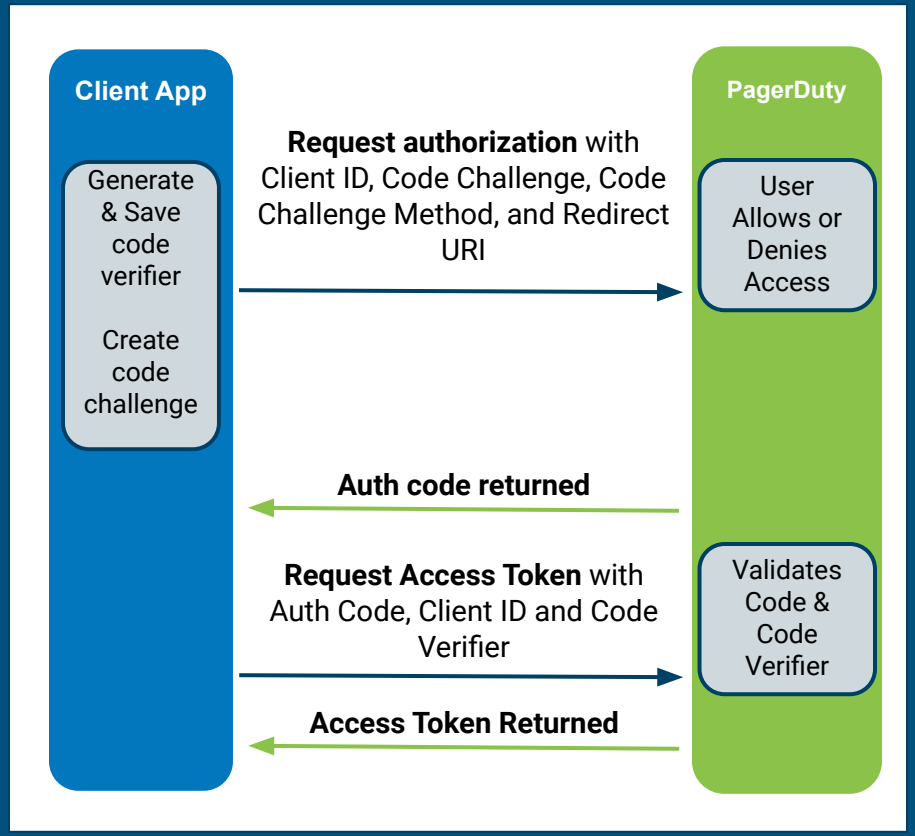
@stmcallister



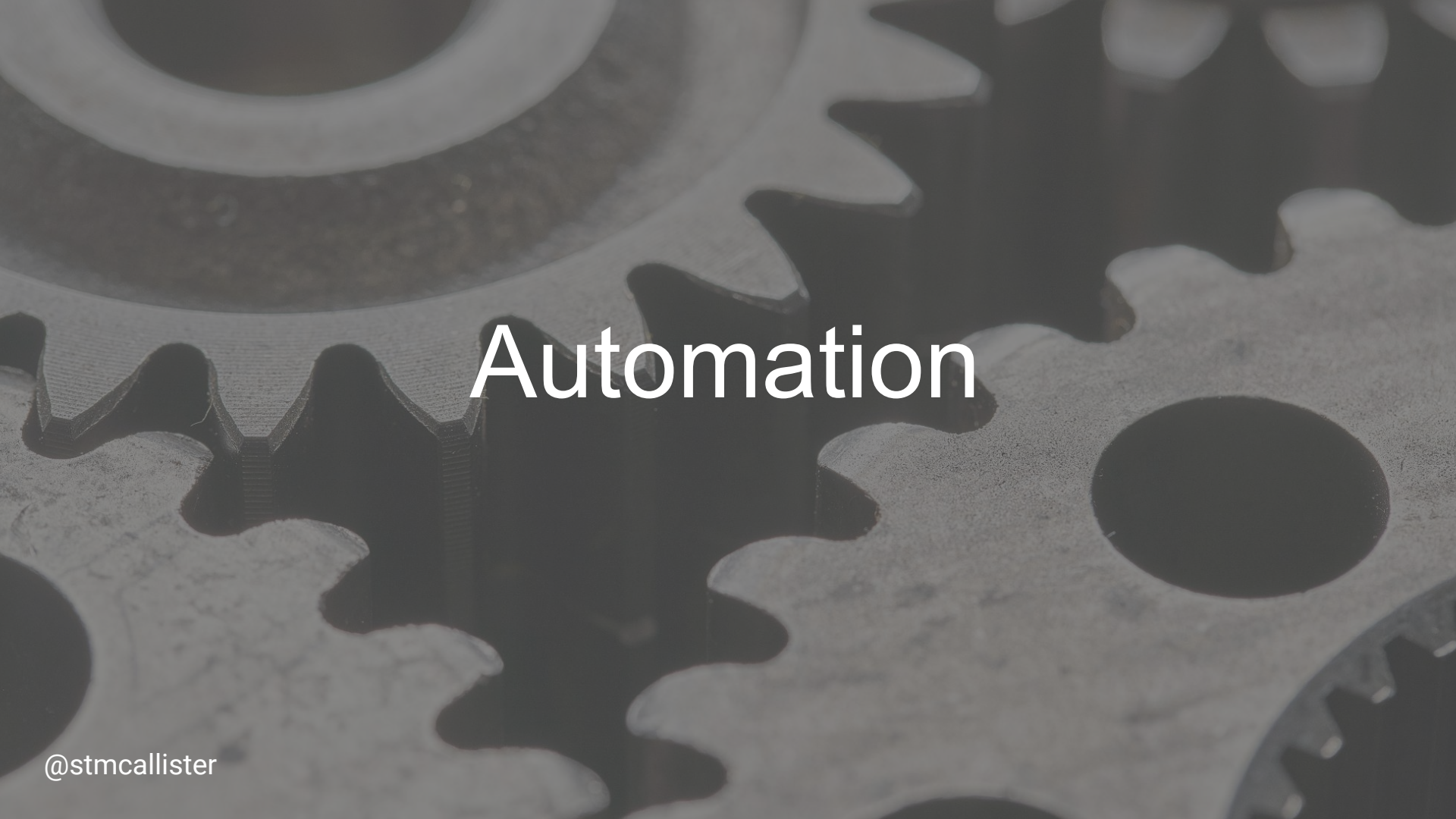
@stmcallister



@stmcallister

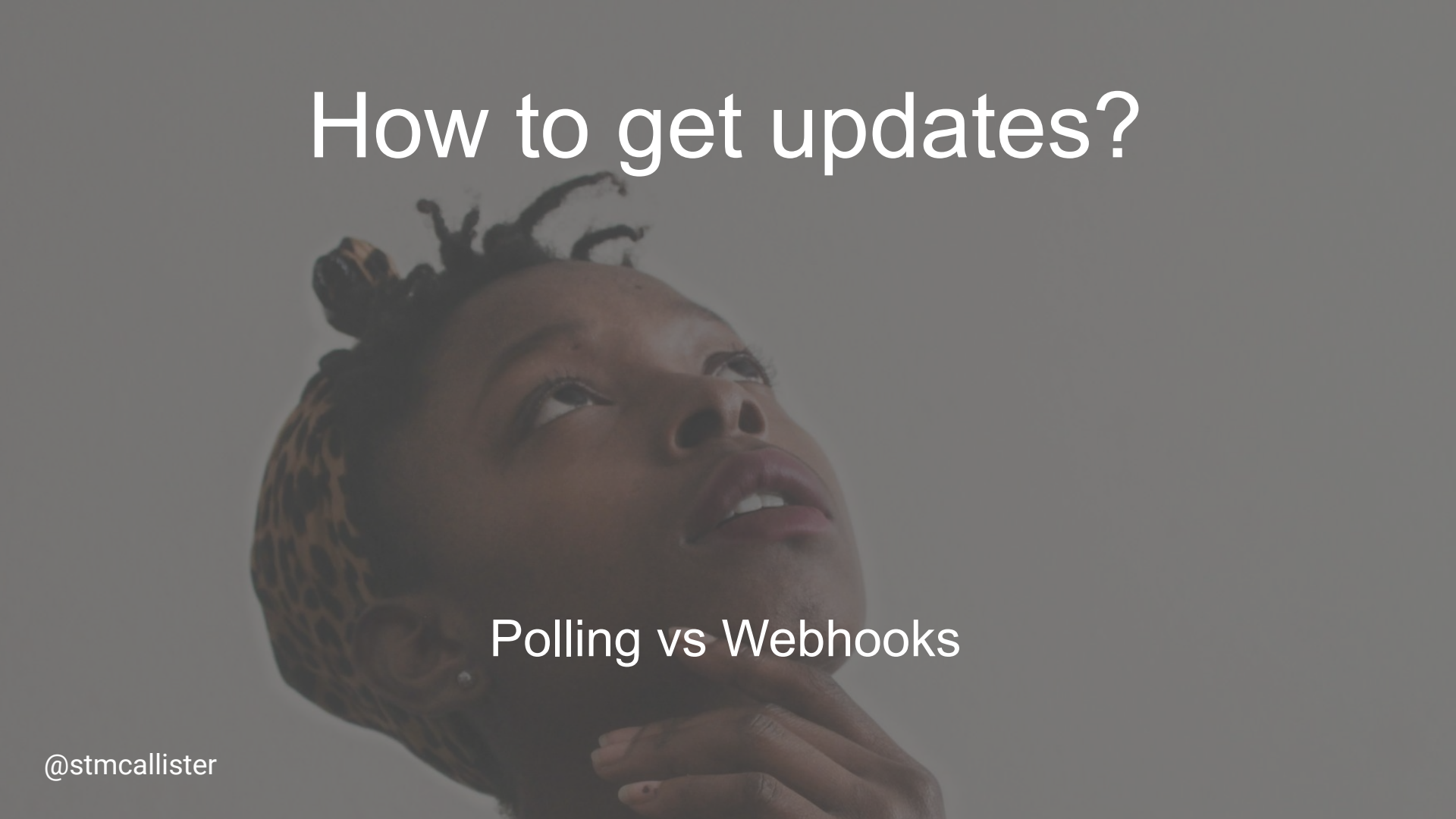


@stmcallister



@stmcallister

How to get updates?



Polling vs Webhooks

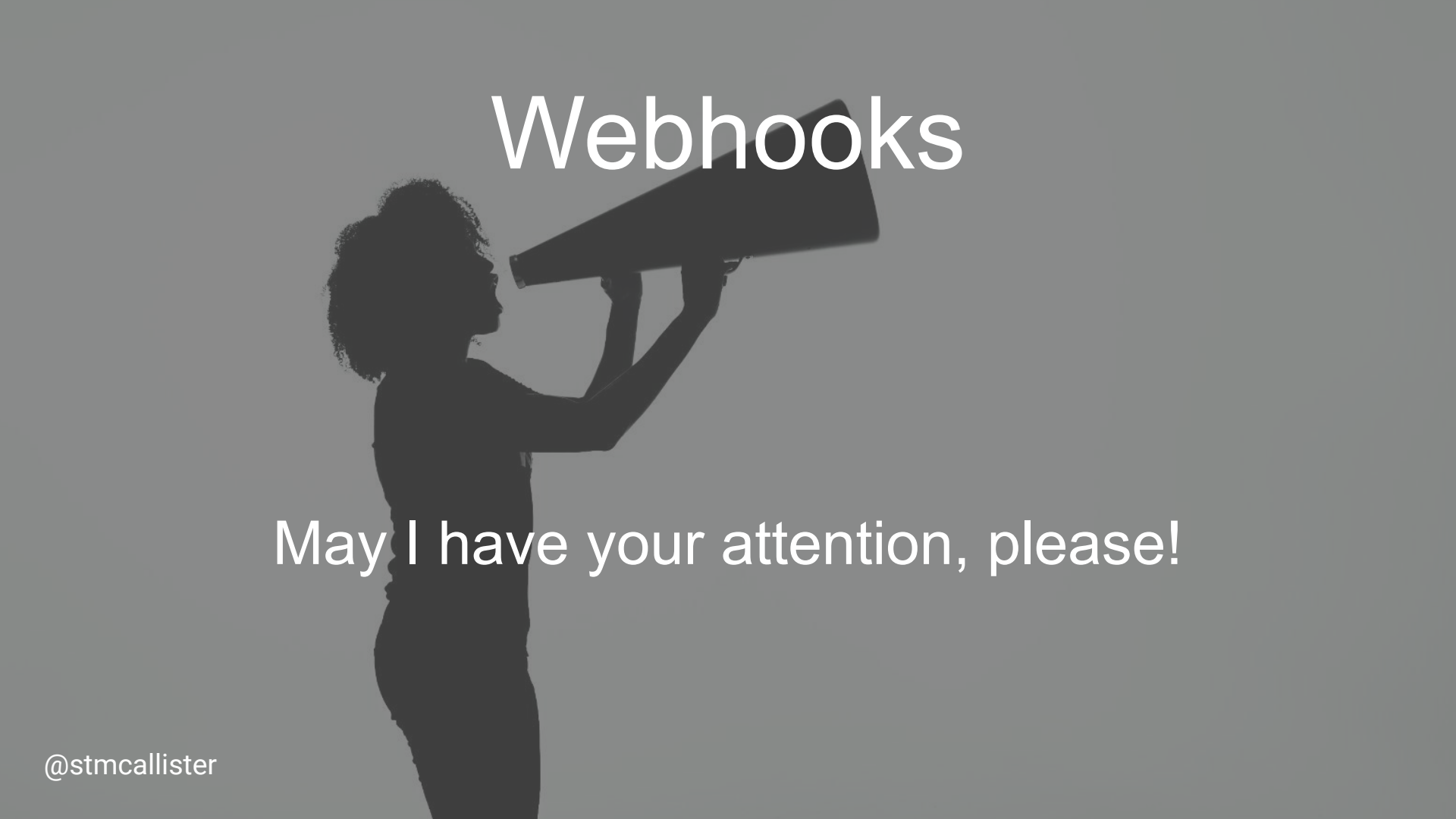
@stmcallister

Polling

Are you done yet?

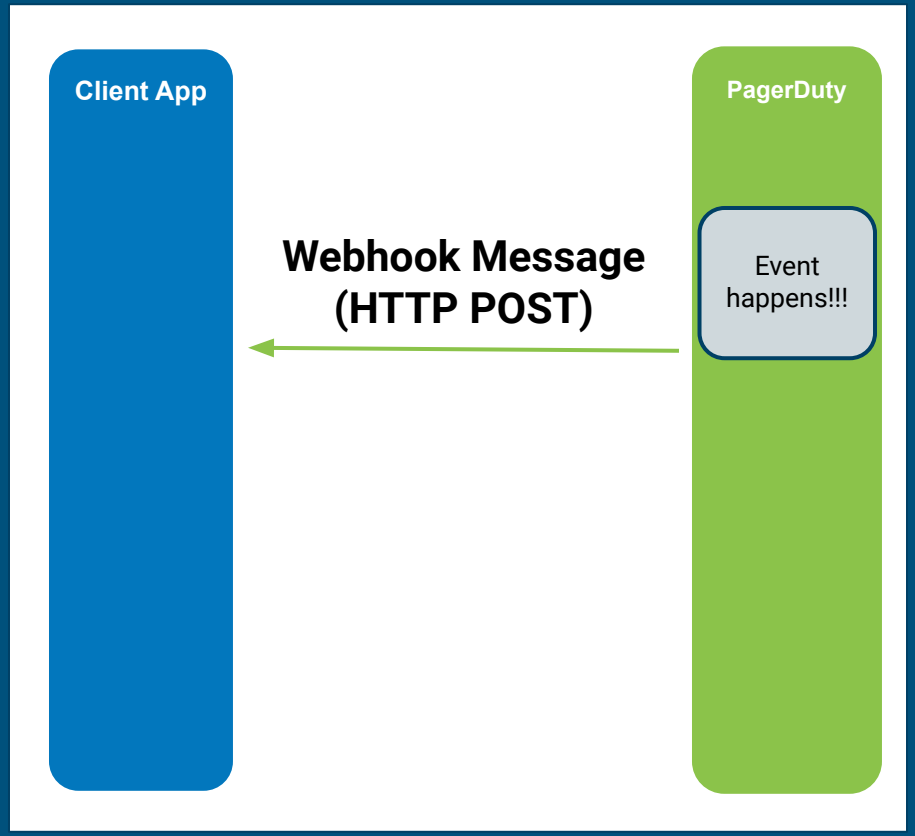
@stmcallister

Webhooks



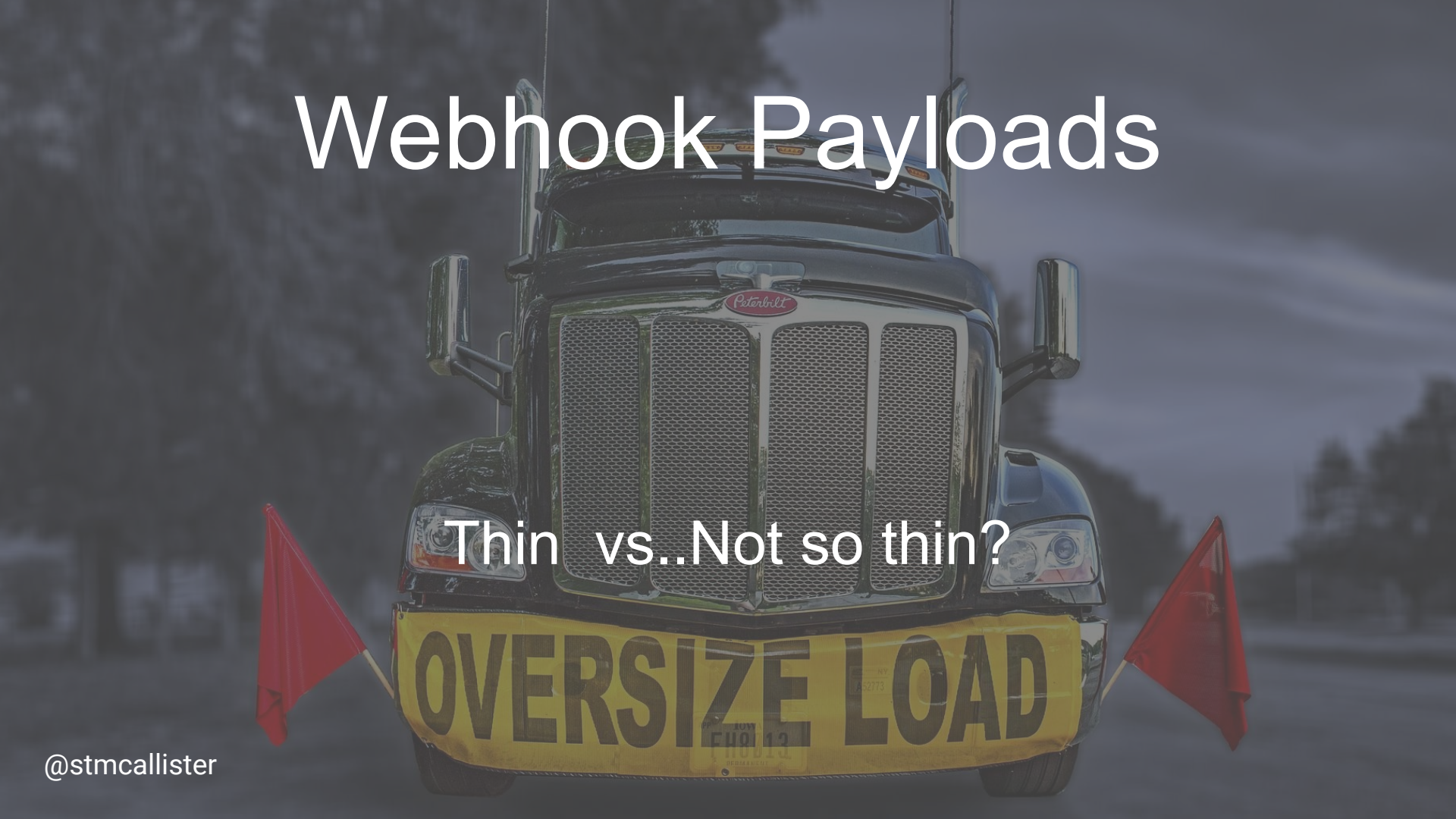
May I have your attention, please!

@stmcallister



@stmcallister

Webhook Payloads



Thin vs..Not so thin?

@stmcallister

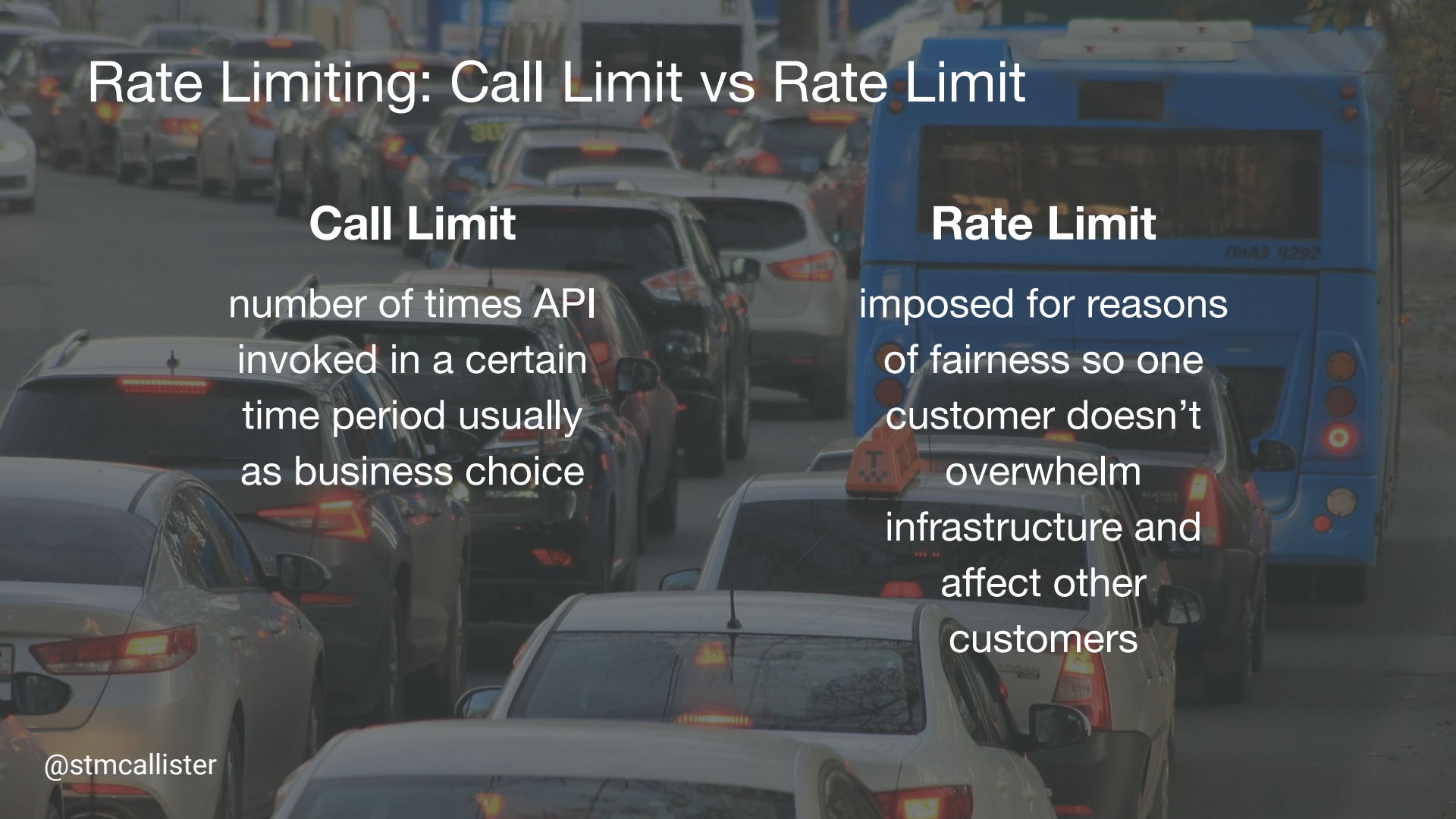
Thin Payload


```
{
  "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
```


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.

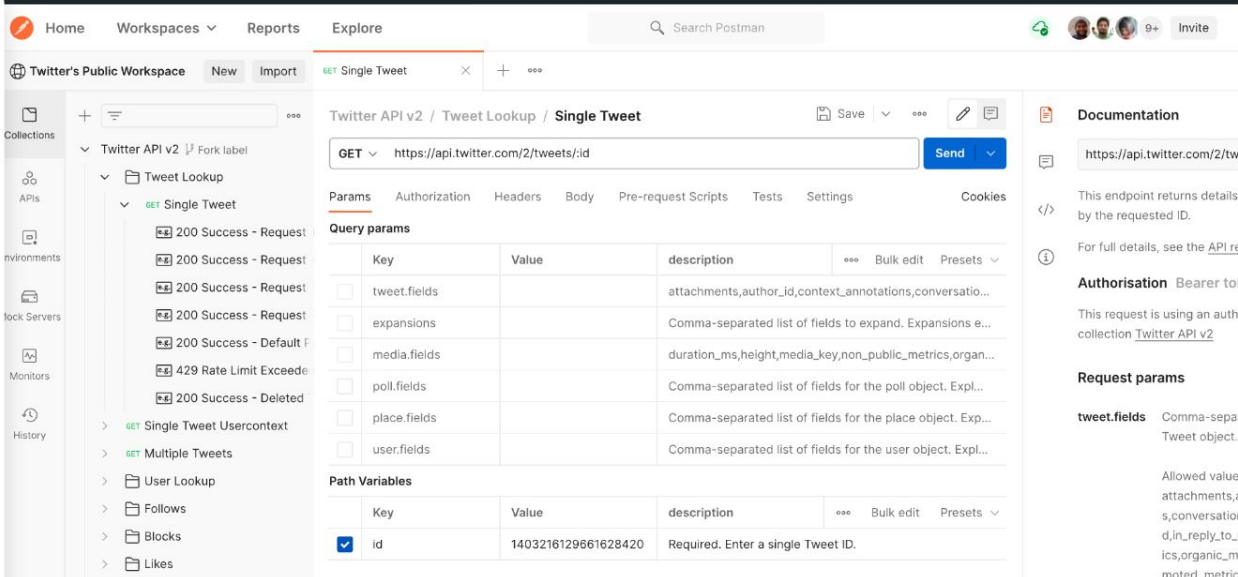
Download the App

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



Scott McAllister

Speaker, Writer, Coder

PagerDuty

stmcallister.github.io

@stmcallister