

Google Cloud Authentication

February 27, 2019 - SIGCSE 2019

Tim Swast <swast@google.com> "Software Friendliness Engineer"

These Slides

bit.ly/gcp-auth-sigcse2019

**[github.com/tswast/code-snippets/tree/master
/2019/python-auth-samples](https://github.com/tswast/code-snippets/tree/master/2019/python-auth-samples)**

Before you begin

1. Select or create a GCP project.



Note: If you don't plan to keep the resources you create in this tutorial, create a new project instead of selecting an existing project. After you finish, you can delete the project, removing all resources associated with the project and tutorial.

[GO TO THE MANAGE RESOURCES PAGE](#)

2. Make sure that billing is enabled for your project.

[LEARN HOW TO ENABLE BILLING](#)

3. Enable the Cloud Vision API.

[ENABLE THE API](#)

4. Set up authentication:



- a. In the GCP Console, go to the **Create service account key** page.

[GO TO THE CREATE SERVICE ACCOUNT KEY PAGE](#)

- b. From the **Service account** drop-down list, select **New service account**.
- c. In the **Service account name** field, enter a name .

GOOGLE_APPLICATION_CREDENTIALS defined in environment but not recognized when authenticating

Ask Question

I am beginner in Python. I am trying to build a sentiment analysis engine using Google's Natural Language service Google' GOOGLE GOOGLE I checked

asked 4 months ago

Google Calendar API 401 "Invalid Credentials"

Some (but not all) Google accounts consistently respond with a 401 when trying to access the Google Calendar API despite tokeninfo telling me the access token I'm using has the proper scope (see curl

asked 2 years ago
viewed 552 times

Google Cloud Storage Upload unauthorized

Ask Question

I'd like to do upload of a file to google cloud storage using javascript, I am using the google api javascript
My bu auth
I tried
So, w
"mess

asked 1 year, 11 months ago

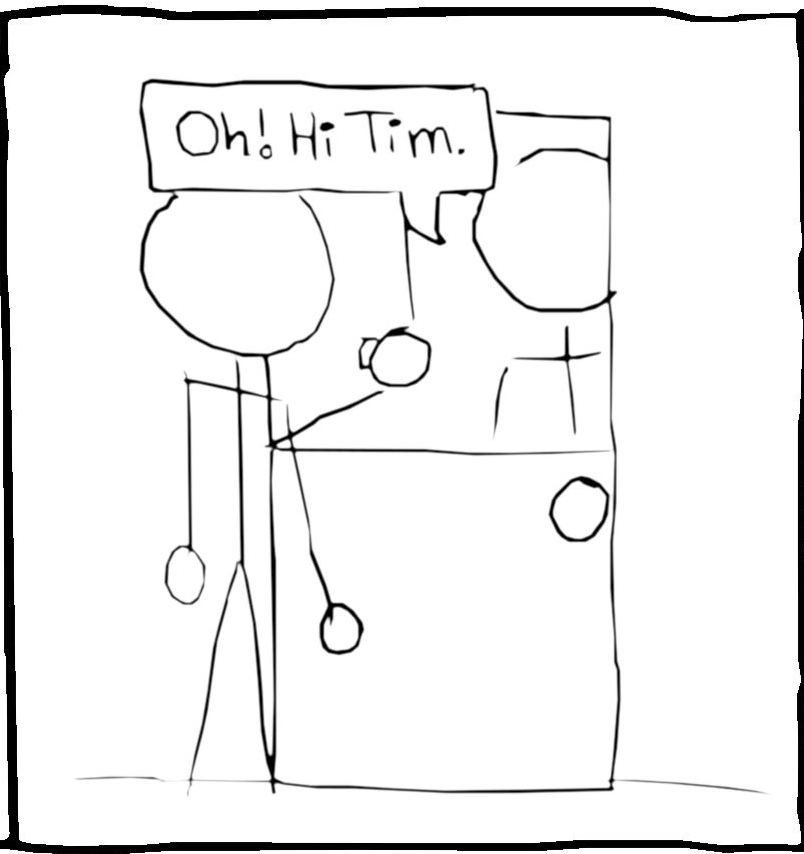
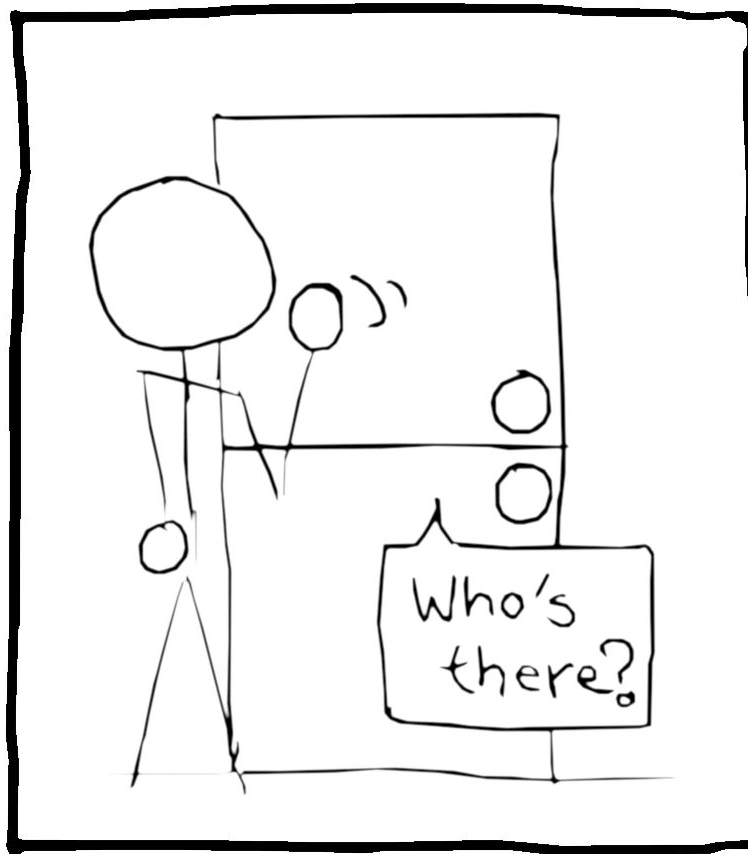
Use Application Default Credentials on Google Compute Engine to access Sheets API

Does the ADC (Application Default Credentials) workflow only support Google Cloud APIs (for example, supports for Google Cloud Storage API, but not the Google Sheet API)?

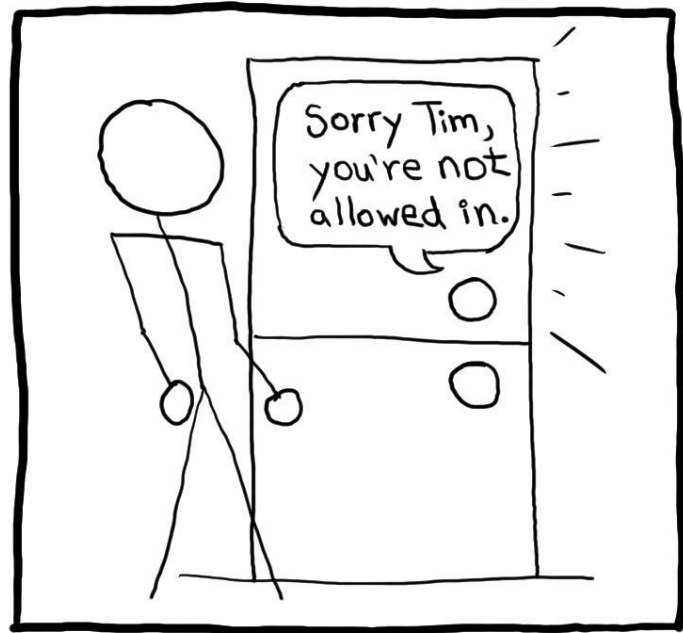
asked 5 months ago
viewed 421 times
active 5 months ago

I'm referring to [google.auth's default method](#) - not having to store any private keys with the code is a great win and the main benefit of making effective use of the ADC (Application Default Credentials) setup.

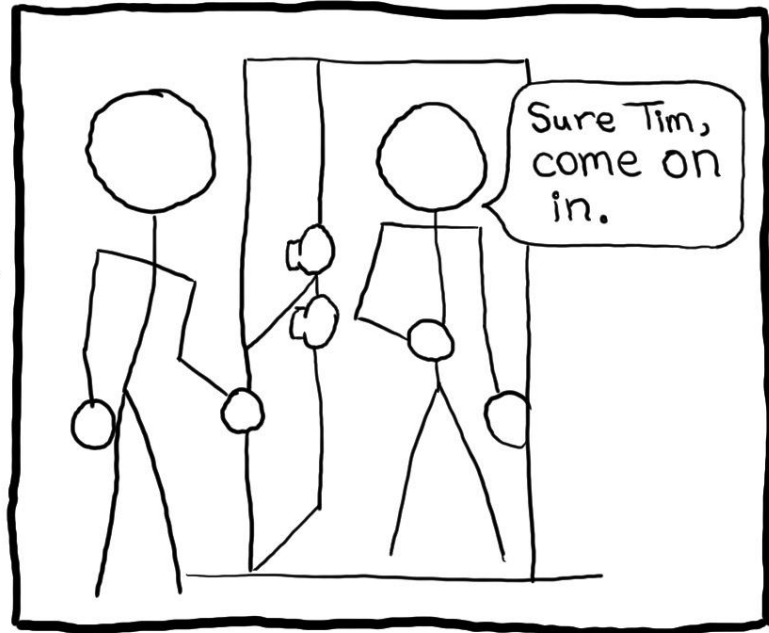
Authentication



Authorization



or



Key Concepts

- **Authentication versus Authorization**
- User accounts
- Access token
- Scopes
- Service accounts
- Identity and Access Management (IAM)

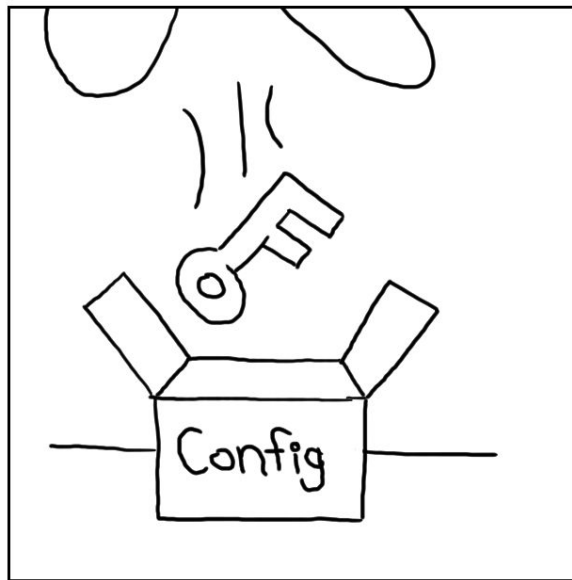
The Problem

Requests to cloud APIs can come from anywhere on the internet.

How does Google know that I'm making a request from *my* app?

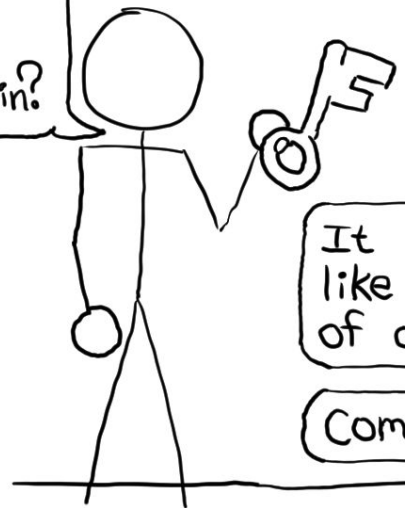
A Simple Authentication Method

API Keys



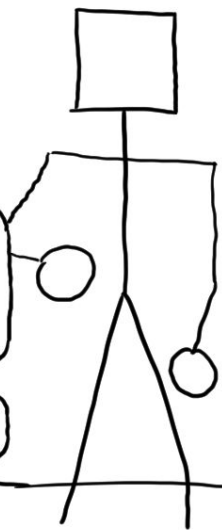
API Keys

I've got
this key.
Can I get in?



It looks
like one
of ours.

Come in.

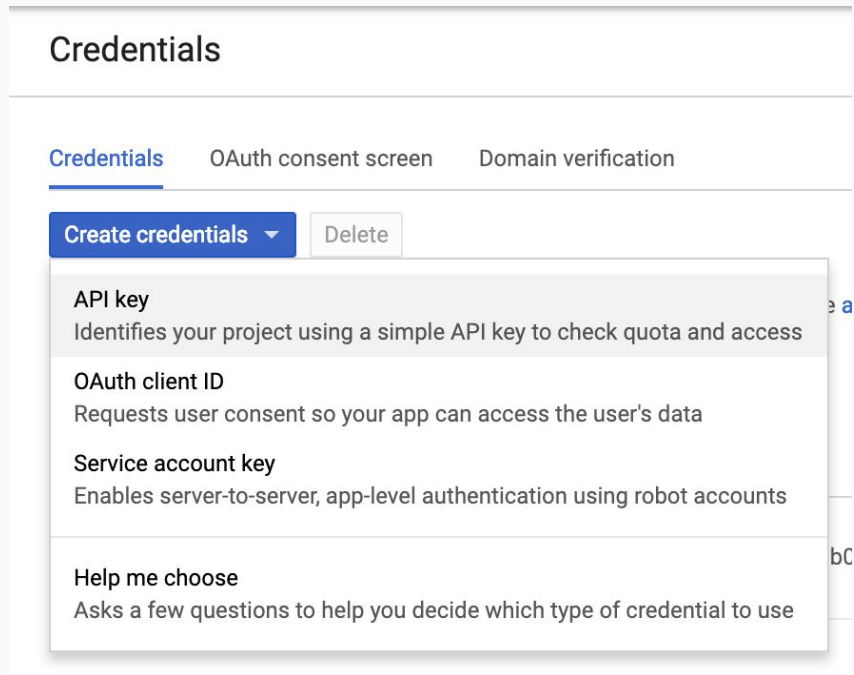
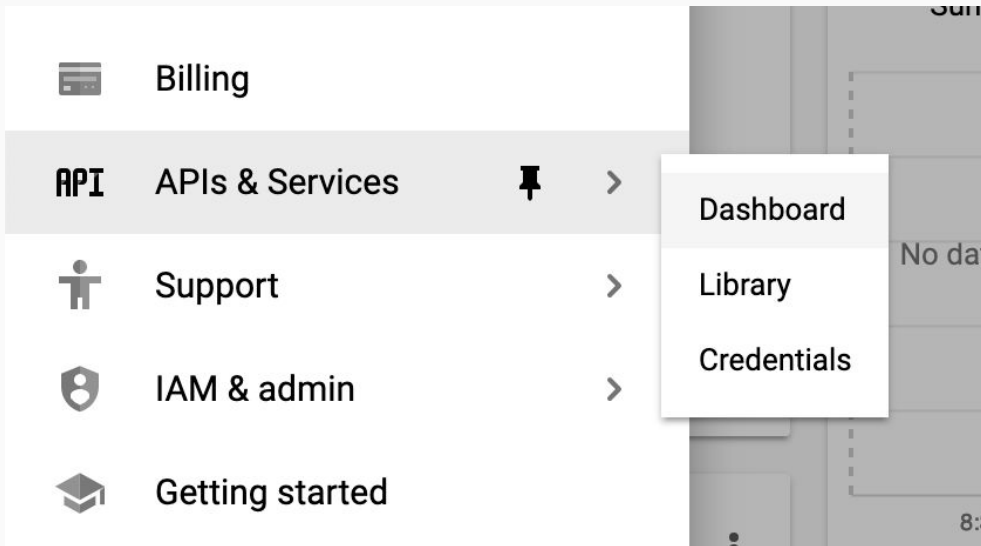


APIs



How are API keys used with
Google APIs?

Getting an API Key



Using an API key with the Google Maps API

GET

https://maps.googleapis.com/maps/api/geocode/json?address=1600+Amphitheatre+Parkway,+Mountain+View,+CA&key=YOUR_API_KEY

Source:

<https://developers.google.com/maps/documentation/javascript/get-api-key>

What if you get the API key wrong?

```
{  
  "error_message" : "The provided API key is invalid.",  
  "results" : [],  
  "status" : "REQUEST_DENIED"  
}
```

Authentication failed!

Authorization

1. **Is the API enabled on the project?**
2. ?
3. ?



Geocoding API

Google

Convert between addresses and geographic coordinates.

ENABLE

Type

[APIs & services](#)

Overview

Convert addresses into geographic coordinates (geocoding), which

What if you don't enable the API?

```
{  
  "error_message" : "This API project is not authorized  
to use this API.",  
  "results" : [],  
  "status" : "REQUEST_DENIED"  
}
```

Authorization failed!

Why can't it be this simple?

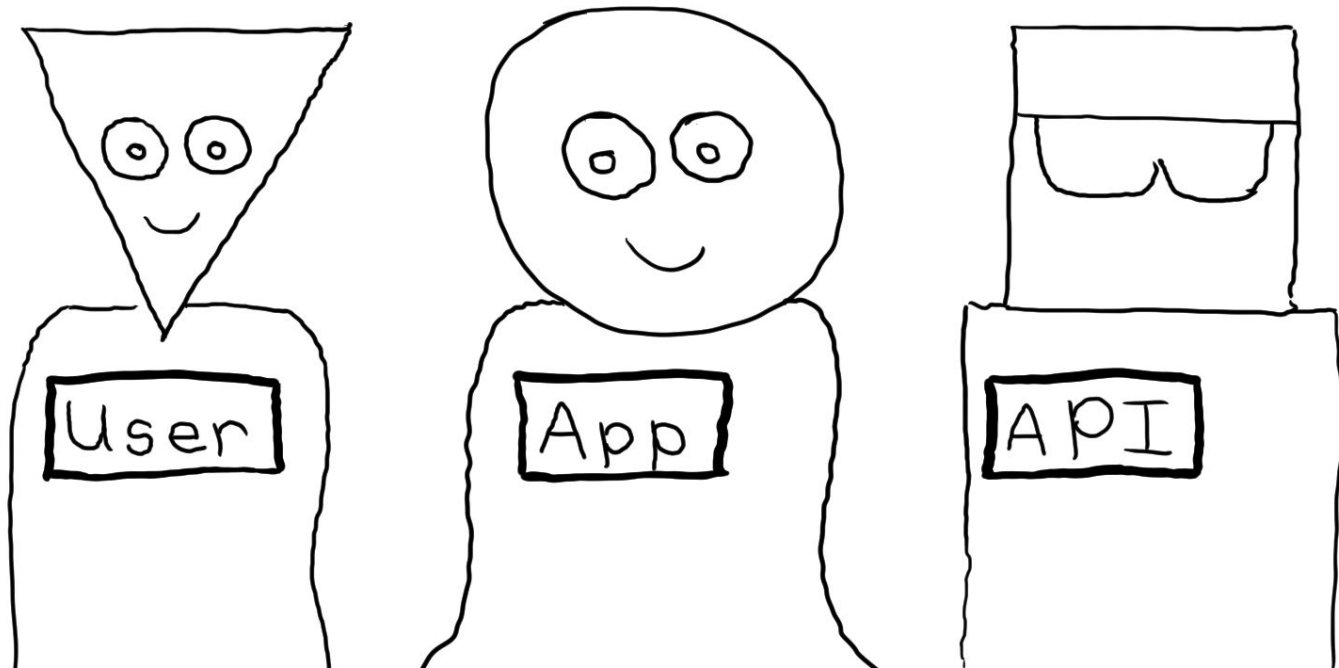
Problems with API Keys

- No expiration. Need to be manually revoked.
- Generally considered insecure (especially compared to the alternatives).
 - Don't check into GitHub! Except sometimes you can't avoid it (like in a single-page web app).

Limitations of API Keys

- Can only be used to access *public* data.
For example, public info on Google Maps.
- Why not private resources?
API keys identify an *app*, not a *user account*.

The Cast



User Accounts

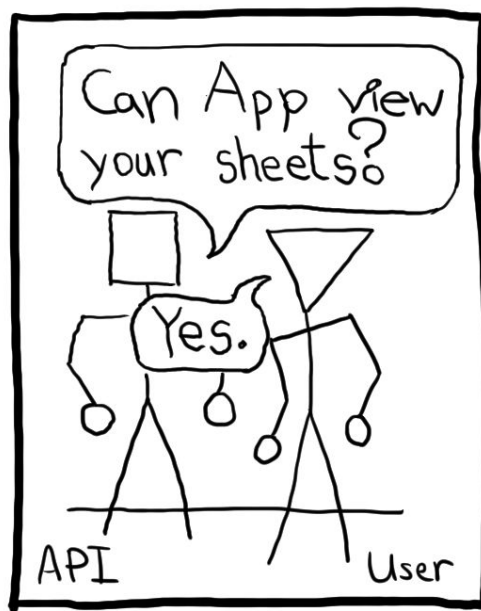
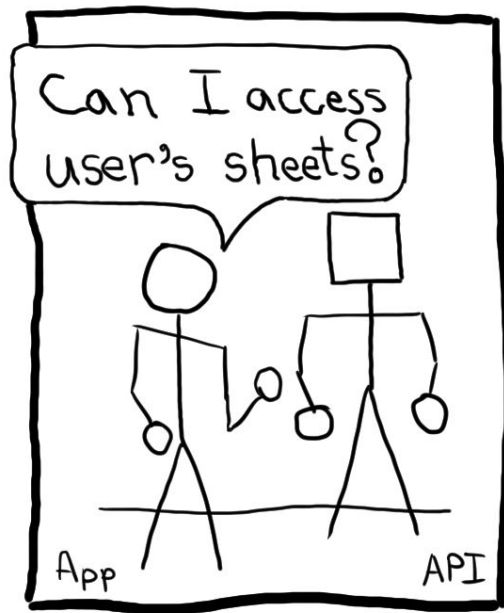
- example@gmail.com
- gsuite.user@example.com
- no.gmail@another-example.com
- 12345-compute@my-project.iam.gserviceaccount.com

Key Concepts

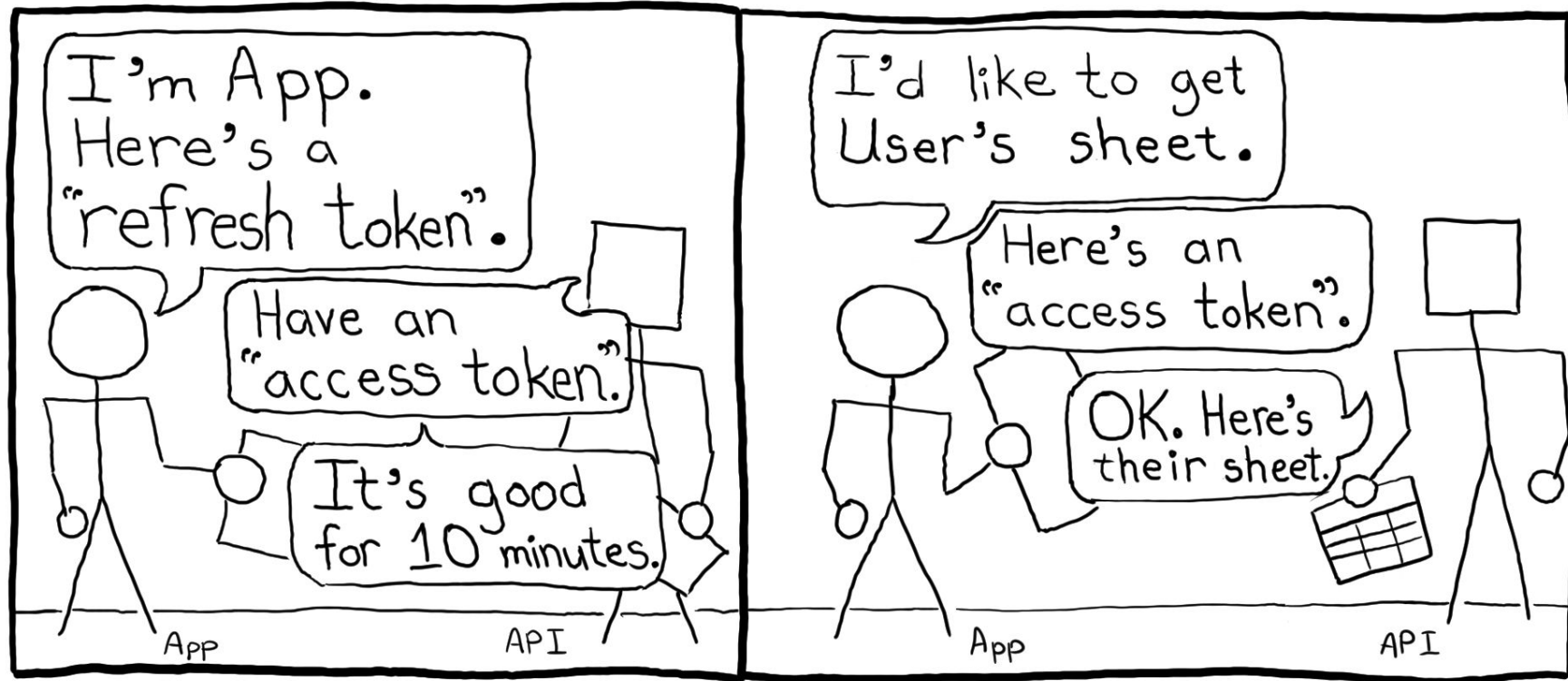
- Authentication versus Authorization
- **User accounts**
- Access token
- Scopes
- Service accounts
- Identity and Access Management (IAM)

How can an app access
non-public user data?

The Flow



Authorization

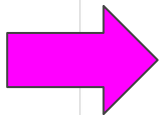


Key Concepts

- Authentication versus Authorization
- User accounts
- **Access token**
- Scopes
- Service accounts
- Identity and Access Management (IAM)



 Sign in with Google



Tim's Test Project wants to
access your Google Account



@gmail.com

This will allow **Tim's Test Project** to:



View your Google Spreadsheets



Make sure you trust Tim's Test Project


You may be sharing sensitive info with this site or app.
Learn about how Tim's Test Project will handle your data by
reviewing its terms of service and privacy policies. You can
always see or remove access in your [Google Account](#).

[Learn about the risks](#)


[Cancel](#)

[Allow](#)

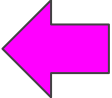
Use *scopes* to choose which of the user's resources the app is allowed to access.

 Sign in with Google

Tim's Test Project wants to access your Google Account

 @gmail.com

This will allow **Tim's Test Project** to:

- View your Google Spreadsheets 

Make sure you trust Tim's Test Project

You may be sharing sensitive info with this site or app. Learn about how Tim's Test Project will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your [Google Account](#).

[Learn about the risks](#)

[Cancel](#) [Allow](#)

Authorization

1. Is the API enabled on the project?
- 2. Did the application request the right scopes?**
3. ?

What happens if you request the wrong scopes?

```
{  
  "error": {  
    "code": 403,  
    "message": "Request had insufficient  
authentication scopes.",  
    "status": "PERMISSION_DENIED"  
  }  
}
```

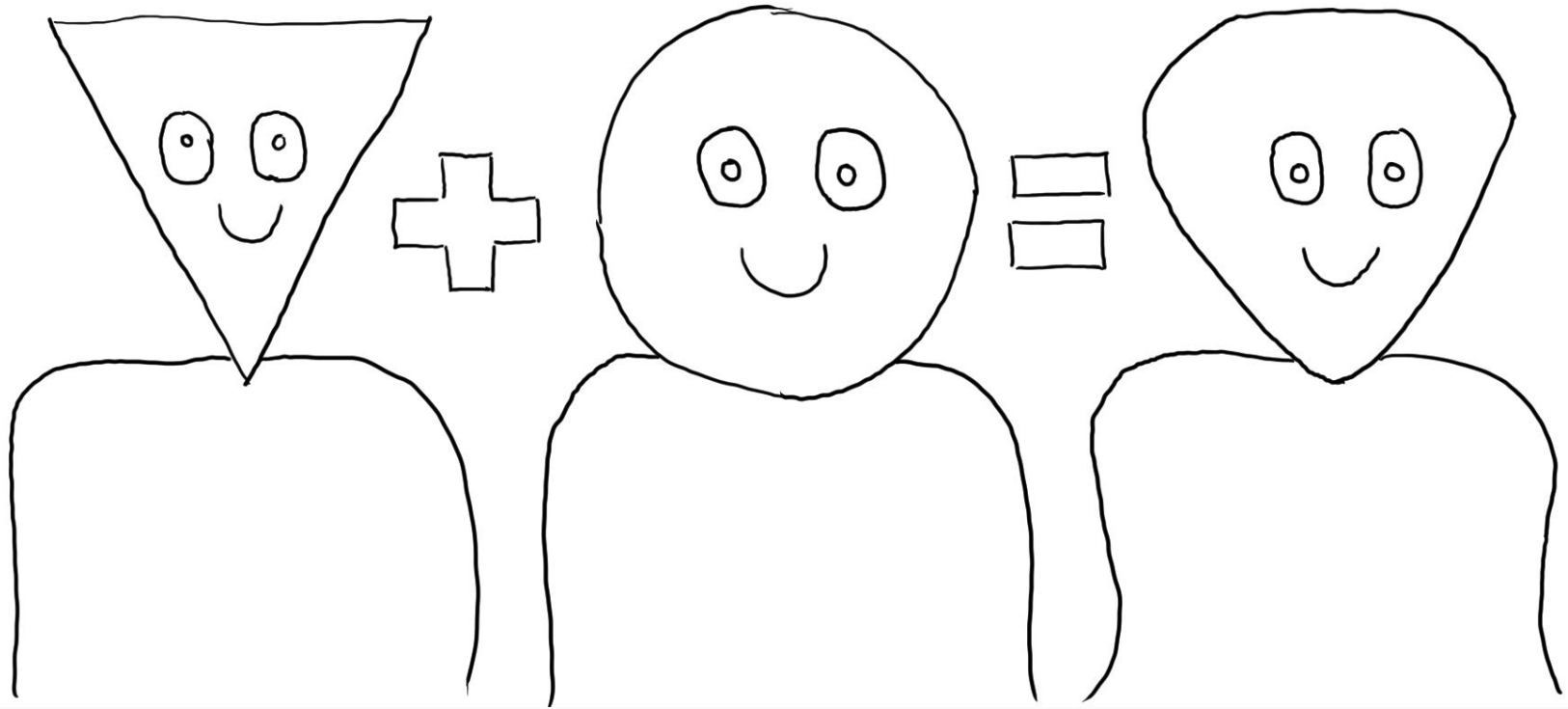
Key Concepts

- Authentication versus Authorization
- User accounts
- Access token
- **Scopes**
- Service accounts
- Identity and Access Management (IAM)

Do I really need to do this flow?

- For most apps deployed to Google Cloud Platform, **No!**
- Usually you don't want to access the *end user's* resources, you want to access *your* resources.

Service Accounts



Google Cloud Platform

Demo Project

Home

Marketplace

Billing

APIs & Services

Support

IAM & admin

Getting started

Security

COMPUTE

App Engine

Compute Engine

Kubernetes Engine

Cloud Functions

STORAGE

Compute Engine

CPU (%)

1 PM

8e-4

Engine

ests/sec)

IAM

Identity & Organization

Organization policies

Quotas

Service accounts

Labels

Privacy & Security

Settings

Cryptographic keys

Identity-Aware Proxy

Roles

Audit Logs

Manage resources

Google Cloud Platform

Demo Project

IAM & admin

Service accounts

+ CREATE SERVICE ACCOUNT

SHOW INFO PANEL

Service accounts for project "Demo Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more](#)

Filter table

	Email	Name ↑	Description	Key ID	Actions
<input type="checkbox"/>	bigquery-qwiklab@tim-swast-demo.iam.gserviceaccount.com	bigquery-qwiklab		No keys	<div></div>
<input type="checkbox"/>	699086934005-compute@developer.gserviceaccount.com	Compute Engine default service account		No keys	<div></div>

Authorization



Key Concepts

- Authentication versus Authorization
- User accounts
- Access token
- Scopes
- **Service accounts**
- Identity and Access Management (IAM)

How to get an access token?

Service account on a local (dev) machine

- Download a key file. Keep it safe!
- Use it to create signed JWTs (use one of the recommended libraries).
- Exchange a signed JWT for an access token.

Review: How to get an "access token"?

- "The Flow", then exchange a refresh token.
- Download a key, sign a JSON Web Token (JWT) message with the key, and exchange.
- Many more options! See Google oauth2l source code for examples.

Authorization

1. Is the API enabled on the project?
2. Did the application request the right scopes?
- 3. Does the user have the right permissions on the resource? (IAM)**



38

- How to get an access token?
Service account on a local (dev) machine
- Download a key file. Keep it safe!
 - Use it to create signed JWTs (use one of the recommended libraries)
 - Exchange a signed JWT for an access token.

39

1

- Review: How to get an "access token"?
- End-user auth: Exchange a refresh token.
 - Local service account: Exchange a signed JSON Web Token (JWT) for an access token.
 - Many more options! See Google oauth2l source code for examples.

40

- Authorization
1. Is the API enabled on the project?
 2. Did the application request the right scopes?
 3. Does the user have the right permissions on the resource? (IAM)

41

1

- Identity and Access Management (IAM)
- Provide fine-grained access control to resources via "roles"
 - Assign a user (or group) a role, associated with a specific resource
 - Examples:
 - There is an "Admin" role and can write object to Cloud Storage Bucket "my-bucket"
 - Data Science Team Google Group is an "Data reader" role and can read from BigQuery tables in "my-project"

42

- Key Concepts
- Authentication versus Authorization
 - User accounts
 - Access tokens
 - Scopes
 - Service accounts
 - Identity and Access Management (IAM)

43

- Scopes for Service Accounts
- Scopes still apply when using service accounts, but are less relevant.
 - When you need fine-grained permissions, create a new service account and assign it the minimum IAM permissions.

Share "Authentication Module for SIGCSE 2019 (go/auth-sli..."

macbook@swast-scratch.iam.gserviceaccount.com X

Add names or email address

View ▼

Message

☐ Skip sending notification

WHO HAS ACCESS

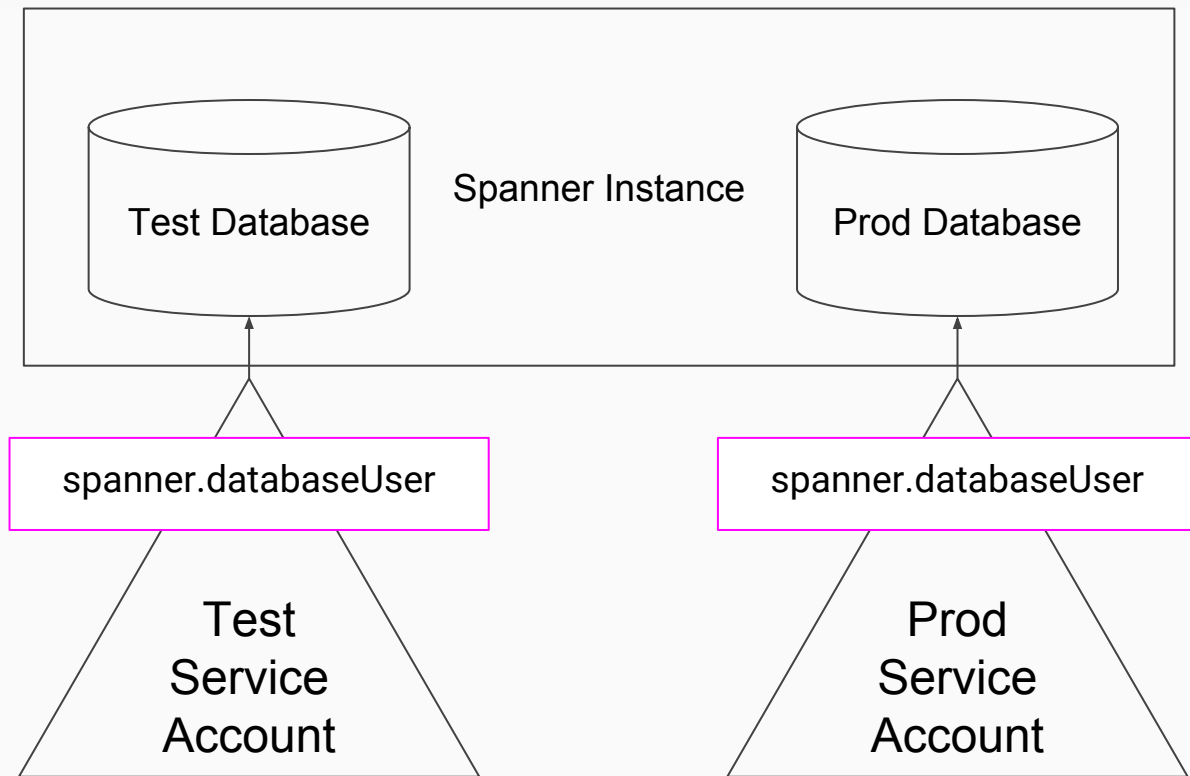
CANCEL

SEND

Identity and Access Management (IAM)

- An IAM *role* is a set of *permissions*.
- A **user** (or group) is assigned a **role**, associated with a **resource**.
- Examples:
 - Tim is an "object writer" role and can write object to Cloud Storage Bucket "my-bucket".
 - Data Science Team Google Group is an "data reader" role and can read from BigQuery tables in "my-project".

Why do we need IAM when we have API enablement and Scopes? Example Project



What happens if you don't have the right IAM permissions?

```
{  
  
  "error": {  
    "code": 403,  
    "message": "acct@my-project-id.iam.gserviceaccount.com <- Account  
does not have storage.objects.get access to <- Permission  
bucket-you-cant-access/README.txt." <- Resource  
  }  
}
```

Key Concepts

- Authentication versus Authorization
- User accounts
- Access token
- Scopes
- Service accounts
- **Identity and Access Management (IAM)**

Resources

- Google Cloud Authentication Guide
`cloud.google.com/docs/authentication`
- oauth2l - command-line tool with every auth method
`github.com/google/oauth2l`
- The OAuth 2.0 Book
`oauth2simplified.com`

Lab: Using Service Accounts to Authenticate

bit.ly/gcp-service-accounts-lab

- **Complete "Setup" section.**
- **Skip to "Access BigQuery from a Service Account" section.**

Questions?

Feel free to contact me.

I'll be available at the Google Booth for most of the conference.

Email swast@google.com

Twitter [@TimSwast](https://twitter.com/TimSwast)

Appendix

Resources : Recommended libraries

- Use the Google Cloud client libraries for your preferred language.
- Google Auth for Python
github.com/googleapis/google-auth-library-python
- Google Auth for Java
github.com/googleapis/google-auth-library-java
- Google Auth for Node.js
github.com/googleapis/google-auth-library-nodejs
- Similar libraries exist for other languages.

Appendix : OAuth 2.0 "Scopes"

Google API Scopes

bit.ly/google-scopes

Appendix :

Protocol details

Using an access token

Protocol details: Use token to call Google API

Example: Making a request to the Cloud Vision API

```
https://vision.googleapis.com/v1/images:annotate
```

HTTP Header:

```
Authorization: Bearer YOUR_ACCESS_TOKEN
```


Protocol details: Use token to call Google API

Example: Making a request to the Cloud Vision API

`https://vision.googleapis.com/v1/images:annotate`

HTTP Header:

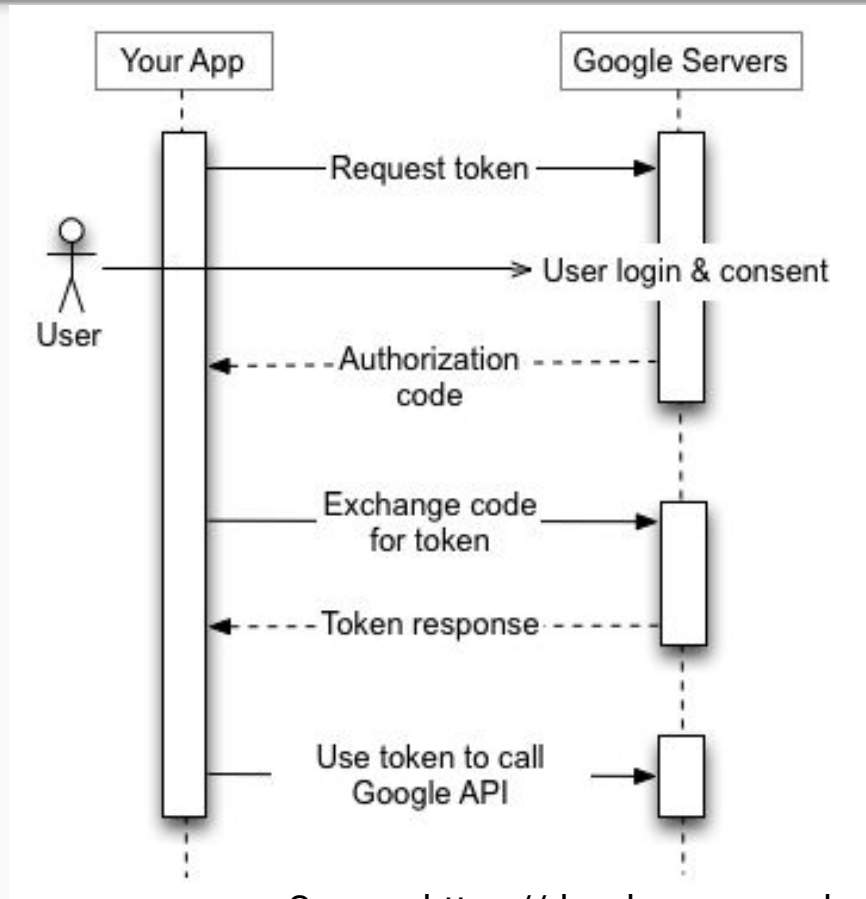
Authorization: Bearer YOUR_ACCESS_TOKEN

Appendix :

Protocol details

Getting an access token

OAuth 2.0 Protocol



Source: <https://developers.google.com/identity/protocols/OAuth2>

Protocol: Service account on a local machine

developers.google.com/identity/protocols/OAuth2ServiceAccount

- Create and sign a JSON Web Token (JWT) using the private key.
- Request a token, including the JWT as the "assertion".

Service account on Google Cloud Platform

Contact "metadata server".

cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#applications

Protocol: Metadata Server

- HTTP GET
`http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token`
- Google Compute Engine / Google App Engine / Google Kubernetes Engine / Google Cloud Functions returns an access token corresponding to the service account the app is associated with.

API keys

bit.ly/problems-with-api-keys

Appendix : Billing

Authorization

1. Is the API enabled on the project?
2. Did the application request the right scopes?
3. Does the user have the right permissions on the resource? (IAM)
4. **Does the project have billing enabled if needed for the API?**

Billing \cap Authentication

- Google requires a *project* in order to bill for API usage.
- Some APIs bill based on the *credentials*.
 - Service Account: bill the project that owns the service account.
 - End-user Credentials: bill the project the owns the "app" (client ID).
 - API key: bill the project that created the API key.
- Some APIs bill based on the *resource* path.
 - Bill the project that owns the resource.
 - e.g. Bill the project that runs your BigQuery query job. User (service account or end-user account) requires the bigquery.jobs.create IAM permission.

Managing Billing Accounts

Users	Projects
Can <i>administer</i> zero or more billing account(s).	There is (at most) 1 billing account <i>associated</i> with a project.

Appendix :

End-user accounts in my app

What if I want users to log in to my app? (Authentication)

Firebase Authentication and Cloud Identity for Customers and Partners (CICP)

- An SDK which provides end-user login,
- Built on OAuth 2.0 for authentication,
- And OpenID Connect to identify the user.

How do I implement user permissions (Authorization)

Firestore and Firebase Real-time Database provide "Role-based Access" controls.

Resource: /stories/{storyid}

```
{
  title: "A Great Story",
  content: "Once upon a time ...",
  roles: {
    alice: "owner",
    bob: "reader",
  }
}
```