Choosing an Authentication Method

cloud.google.com/api-gateway/docs/authentication-method

API Gateway supports multiple authentication methods that are suited to different applications and use cases. API Gateway uses the authentication method that you specify in your service configuration to validate incoming requests before passing them to your API backend. This page provides an overview for each supported authentication method in API Gateway.

API keys

An API key is a simple string that identifies a Google Cloud project for quota, billing, and monitoring purposes. A developer generates an API key in a project in the Cloud Console and embeds that key in every call to your API as a query parameter or in a request header.

If you specify an API key requirement in your API config, API Gateway uses the API key to look up the Google Cloud project that the API key is associated with. API Gateway rejects requests unless the API key was generated in your Google Cloud project or within other Google Cloud projects in which your API has been enabled.

Unlike credentials that use short-live tokens or signed requests, API keys are a part of the request and are therefore considered to be vulnerable to man-in-the-middle attacks and therefore less secure. You can use API keys in addition to one of the authentication methods described below. For security reasons, don't use API keys by themselves when API calls contain sensitive data.

Use case

To use API Gateway features such as quotas, you can pass in an API key so that API Gateway can identify the Google Cloud project that the client application is associated with.

About API key authentication for API Gateway

If you are using an API key for authentication, you must first enable API key support for your service. Enter the following command, where:

- *API_ID* specifies the name of your API.
- *HASH* is the unique hash code generated when you deployed the API.
- *PROJECT_ID* specifies the name of your Google Cloud project.

```
gcloud services enable API_ID-HASH.apigateway.PROJECT_ID.cloud.goog
```

For example:

```
gcloud services enable my-api-a12bcd345e67f89g0h.apigateway.my-project.cloud.goog
```

Service accounts

To identify a service that sends requests to your API, you use a service account. The calling service uses the service account's private key to sign a secure JSON Web Token (JWT) and sends the signed JWT in the request to your API.

Use case

JWTs and service accounts are well suited for microservices. For more information, see Authentication between services.

Rate and review