Why and when to use API keys

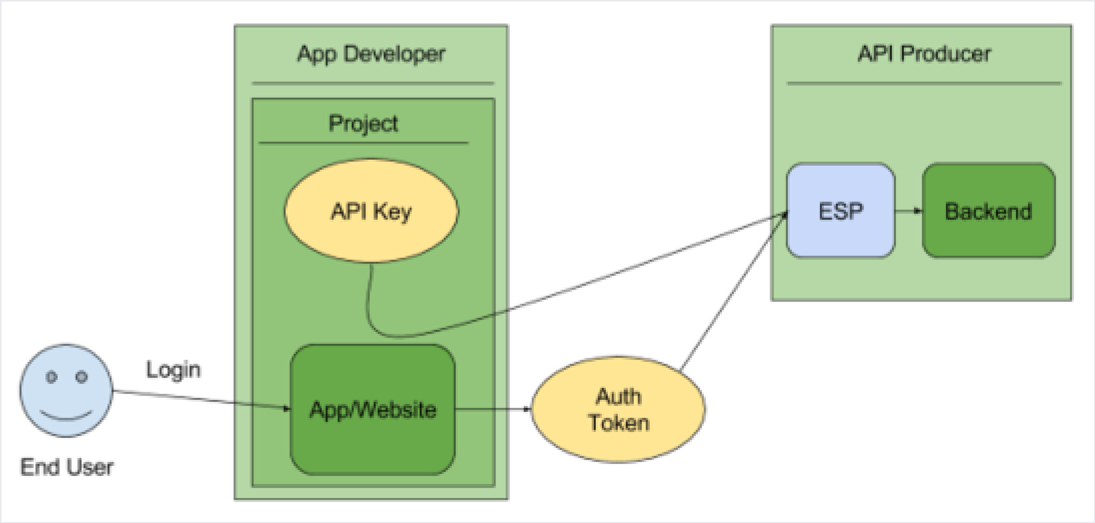
OpenAPI | gRPC (/endpoints/docs/grpc/when-why-api-key)

This page provides background information on API keys and authentication: how each of these are used, the differences between them, and the scenarios where you should consider using API keys.

API keys are for projects, authentication is for users

Cloud Endpoints handles both API keys and authentication schemes, such as Firebase or Auth0. The main distinction between these two is:

- API keys identify the calling project — the application or site — making the call to an API.
- Authentication tokens identify a user — the person — that is using the app or site.



API keys provide project authorization

To decide which scheme is most appropriate, it's important to understand what API keys and authentication can provide.

API keys provide

- **Project identification** — Identify the application or the project that's making a call to this API
- **Project authorization** — Check whether the calling application has been granted access to call the API and has enabled the API in their project

API keys aren't as secure as authentication tokens (see Security of API keys (#security_of_api_keys)), but they identify the application or project that's calling an API. They are generated on the project making the call, and you can restrict their use to an environment such as an IP address range, or an Android or iOS app.

By identifying the calling project, you can use API keys to associate usage information with that project. API keys allow the Extensible Service Proxy (ESP) (/endpoints/docs/openapi/glossary#extensible_service_proxy) to reject calls from projects that haven't been granted access or enabled in the API.

Authentication of users

By contrast, authentication schemes typically serve two purposes:

- **User authentication** — Securely verify that the calling user is who they claim to be.
- **User authorization** — Check whether the user should have access to make this request.

Authentication schemes provide a secure way of identifying the calling user. Endpoints also checks the authentication token to verify that it has permission to call an API. Based on that authentication, the API server decides on authorizing a request.

If you need the ability to identify the user making the call, see Authenticating users (/endpoints/docs/openapi/authenticating-users).

While API keys identify the calling project, they don't identify the calling user. For instance, if you have created an application that is calling an API, an API key can identify the application that is making the call, but not the identity of the person who is using the application.

If you need a more secure way to limit which projects or services can call your API, see Authentication between services (/endpoints/docs/openapi/service-account-authentication).

Security of API keys

API keys are generally not considered secure; they are typically accessible to clients, making it easy for someone to steal an API key. Once the key is stolen, it has no expiration, so it may be used indefinitely, unless the project owner revokes or regenerates the key. While the restrictions you can set on an API key mitigate this, there are better approaches for authorization.

For examples, see Authenticating users (/endpoints/docs/openapi/authenticating-users).

When to use API keys

An API may restrict some or all of its methods to require API keys. It makes sense to do this if:

- You do want to block anonymous traffic. API keys identify an application's traffic for the API producer, in case the application developer needs to work with the API producer to debug an issue or show their application's usage.
- You want to control the number of calls made to your API.
- You want to identify usage patterns in your API's traffic. You can see application usage in APIs & services (http://console.developers.google.com).
- You want to filter logs by API key.

API keys cannot be used for:

- Identifying individual users — API keys don't identify users, they identify projects.
- Secure authorization.
- Identifying the creators of a project.

Service Infrastructure (/service-infrastructure/docs/overview) doesn't provide a method to directly look up projects from API keys.

How to use API keys

To learn how to set up and use API key access, see Restricting access with API keys (/endpoints/docs/openapi/restricting-api-access-with-api-keys).

Last updated 2020-11-16 UTC.