API key vs Oauth authentication

—---------------------------------

Api key –

Disadvantages –

* API Key can be an easy way to enforce some authentication

Many API keys are sent in the query string as part of the URL, which makes it easier to discover for someone who should not have access to it

* 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.
* Api key cannot be used for Identifying individual users — API keys don't identify users, they identify projects ,Secure authorization. Identifying the creators of a project.

Oauth –

Advantages -

* OAuth is more sophisticated with more options but also needs more knowledge to get implemented correctly, not only on the client but also on the server-side
* Use OAuth access tokens if you want users to easily provide authorization to applications without needing to share private data or dig through developer documentation
* Google Cloud APIs use the [OAuth 2.0 protocol](https://tools.ietf.org/html/rfc6749) for authenticating both user accounts and service accounts. The OAuth 2.0 authentication process determines both the principal and the application