OAuth 2.0

# What is OAuth 2.0

Basically it’s an authorization protocol, which allows accessing the resources of the resource owner by enabling a third-party application or called client application (e.g. Google, Facebook or GitHub etc.).

Table

Description automatically generated

There are 4 roles in OAuth:

* The Third-Party Application: "Client"

The client is the application that is attempting to get access to the user's account. It needs to get permission from the user before it can do so. It issues the Access Token which acts like the user’s Driver’s License

* The API: "Resource Server"

The resource server is the API server used to access the user's information.

* The Authorization Server

This is the server that presents the interface where the user approves or denies the request. In smaller implementations, this may be the same server as the API server, but larger scale deployments will often build this as a separate component.

* The User: "Resource Owner"

The resource owner is the person who is giving access to some portion of their account.

In Step 2, user will see the following authorization page (reside in Authorization Server where it sends the authorization request to third party application to initialize the authorization process), this is what OAuth about, user (Resource Owner) authorizes a third party application or client application to get access to its resources (called Resource Server or Resource API since the Authorization Token is provided in the API request header)

Graphical user interface, text, application

Description automatically generated