**OAuth 2.0 – Report**

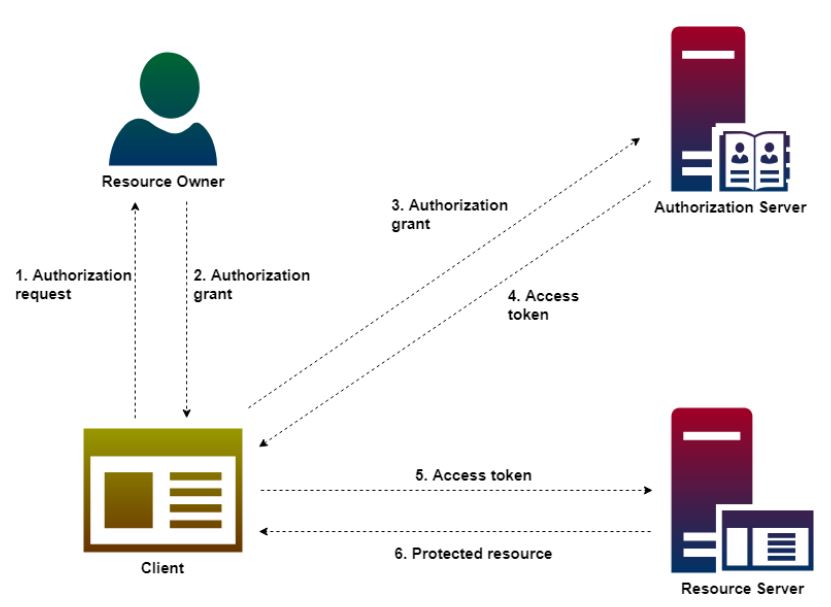
**Introduction**

OAuth means the Open Authorization. This framework mentions how the unrelated servers and services can allow the authenticated access to the resources safely without sharing the initial credentials. OAuth provides the authorization flows for the desktop and web applications as well as mobile devices.

There are 4 roles in OAuth

* Resource Owner
* Client
* Authorization Server
* Resource Server

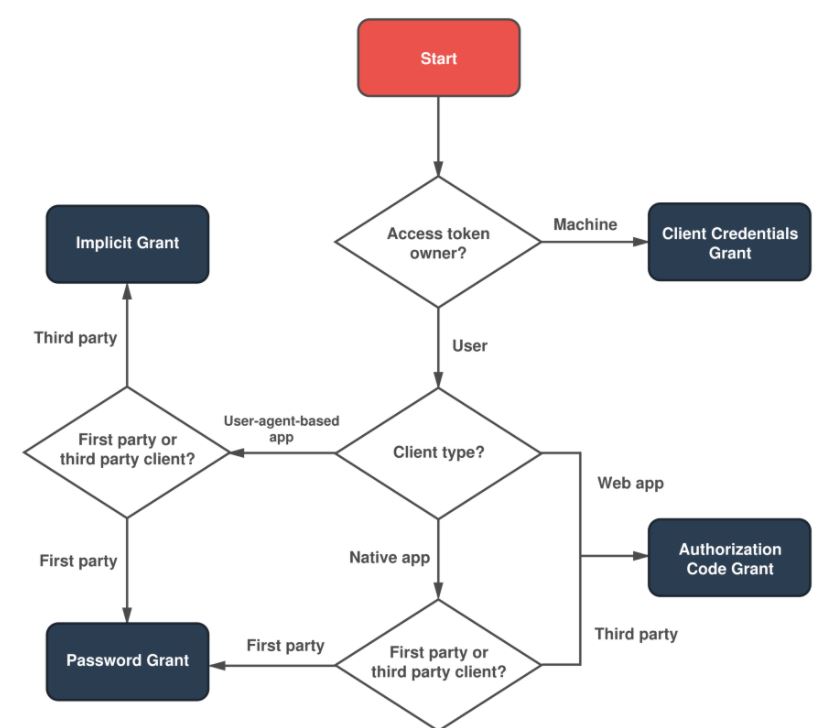
**Abstract Flow of the protocol**

****

**Steps**

1. The application request to access some resources (protected) in the server where the user is authenticated and authorized.
2. Then the application receives an authorization grant if the user authorized the request.
3. Then the application requests an access token from the server (authorization server) by presenting authentication of its own identity.
4. If the authorization grant is valid and the client application’s identity is authenticated, then the authorization server issues an access token to the application.
5. Then the client application requests the resource form the resource server.
6. If the access token is valid, then the resource server serves the resource to the client.

**Grant Types**

****

**Flows to build the OAuth-based client application**

1. Step 1 – Application Registration

Register the application with the service provider. This process is done through the registration form in the “developer” portal. We have to give Application Name, Application website and redirect URI. After the successful registration Google will provide Client ID, and Client Secret.