**Oauth**

Auth stands for Authorization. Oauth was Introduced not to Authorize any Person like in JWT, but it was meant for a Service to authorize another Service. So, it is kind of Standard between Services.

This standard is also called Access Delegation.

Eg.

1. Two services are there say printingApp and GoogleDrive
2. You want to print one of your doc which resides in Google Drive
3. If Oauth is not implemented there is no way printing App can take doc from google drive.
4. If Oauth is implemented then printing app will go to Google asking the doc. Google inturn comes to us asking credentials and showing the permissions that printing app wants.
5. User enter the creds and Google provides a token(JWT) to printingApp which has limited access.
6. So, now every time when the printing app wants to access the information from the Google, it hands over a token to the Google. Google verifies it and allows the printing App to the limited access.

So, that’s wht auth stands for authorization as user is already authenticated to all the services. The problem is the services that needs to get authorized with each other.

Advantages:

1. Token can’t be tempered.

Termonologies of Oauth:

1. **Resource**

* What is the thing that needs to be accessed. Resource is always protected.

1. **Resource** **Owner**

* An entity capable of granting access to a protected resource. So, google user is an Owner.

1. **Resource** **Server**

* Machine/App that is holding the Resource

1. **Client**

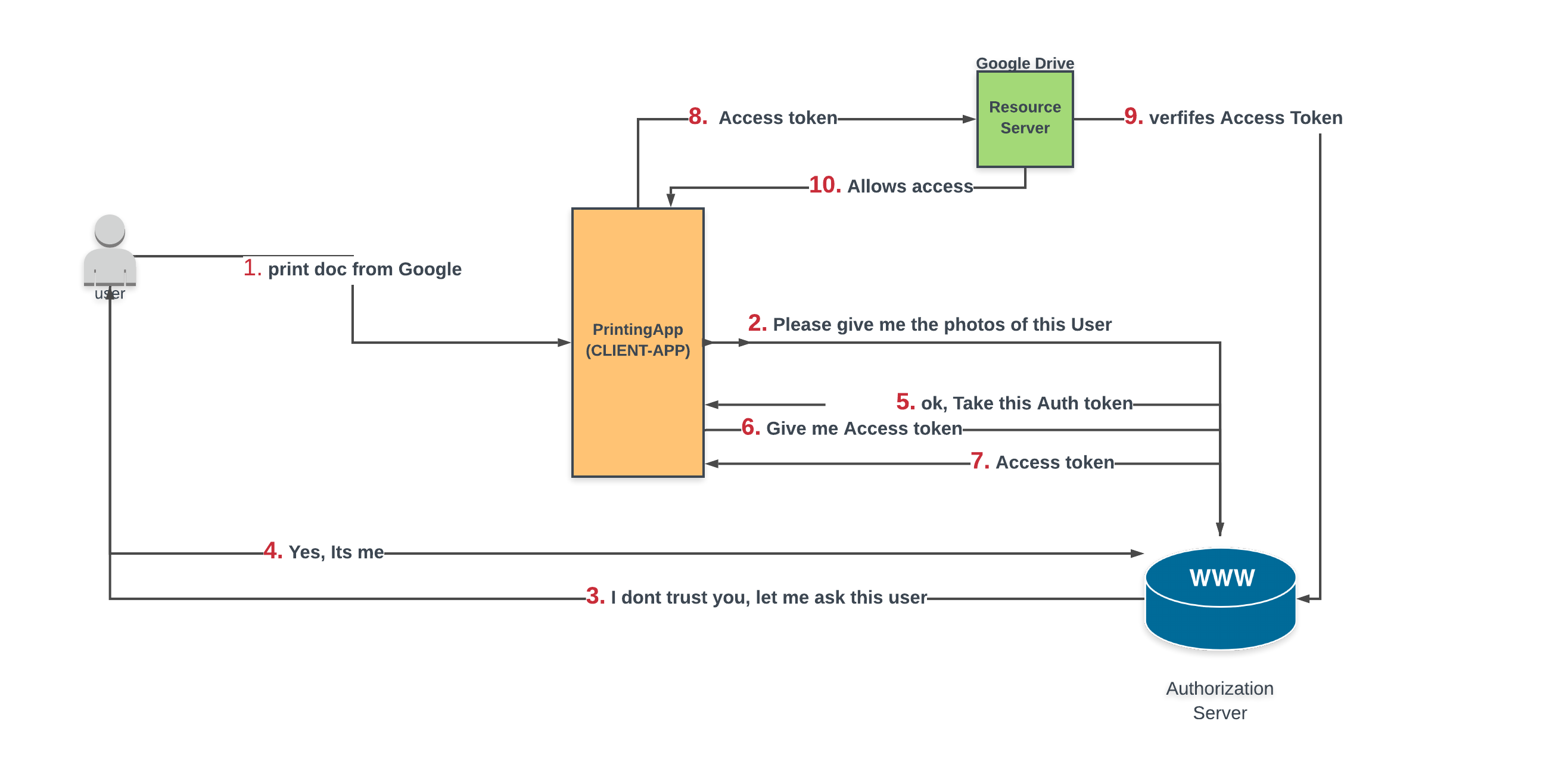
* Client is an Application that needs access to the protected resource on behalf of the Owner. In this case printingApp

So, Google has the responsibility to provide the security to the resource. Typically the Resource Service has Authorization Server with it. As Google has implemented Oath so Authorization server has the responsibilty is to make sure that the suthorization is happening fine. This Authorization Server can be a separate entity or it can be with in the resource server also.

Authorization is the server that issues a token to the client on the behalf of resource server.

There are several flows in Outh

Flow 1.



1. User asks printing App to print doc which is in Google drive
2. Printing App goes to the Authorizaation server of Google and asks the docs
3. Authorization server in turn asks User whether to allow printinApp or not.
4. User allows
5. Authorization server grants Auth token of limited validity to the printing App
6. Printing App again asks Authorization server for Access token to access doc in Google.
7. Autorization server gives access token to printing App
8. Printing app goes to google with the acess token
9. Google again verifies it with the Authorization Server
10. Google allows printing App to access the resource.

Flow 2

Implicit flow: Instead of Auth token, authorization server hands over access token directly to the printing App.