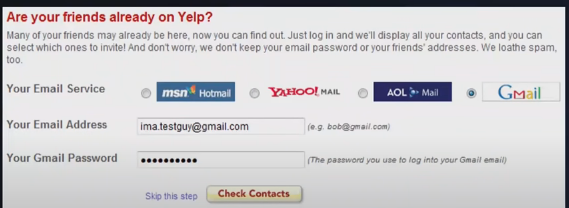
# Before OAuth

In 2009 .. when 1 appn wants to talk to another application like if ticketnew app wants to get all user details that ticketnew application will take the gmail user name and password (which is very bad they can misuse the users gmail id credentials ) and that application will talk to google and get all his information like name, age, mail id, .. ex:- apps book my show





Oauth 2.0 terminology

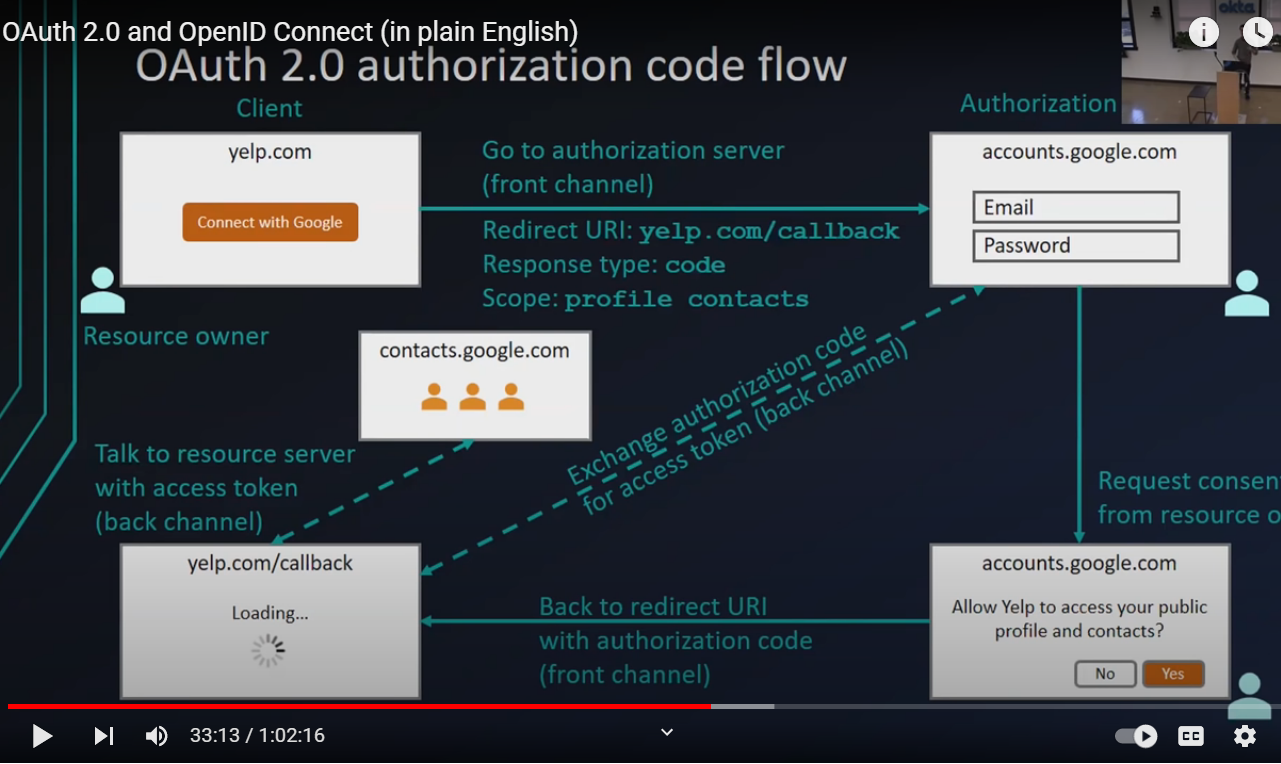
Resource owner :- who owns the data it is the person who has the data , ex:- we

Authorization server :- Is one who provides authorization token ,access toke

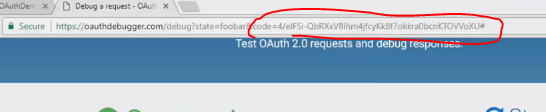
Resource server:- where the resource is like google contacts api

Google contacts API is reusable secured API, if u want to use it authorization is mandatory, and

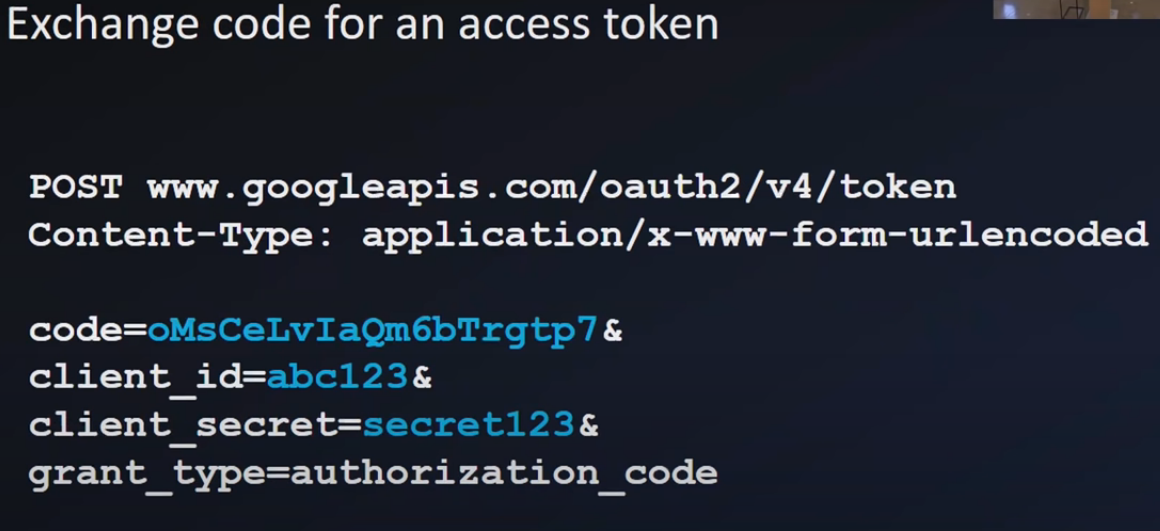
Similarly if u want to develop an reusable service ur api also should implement security



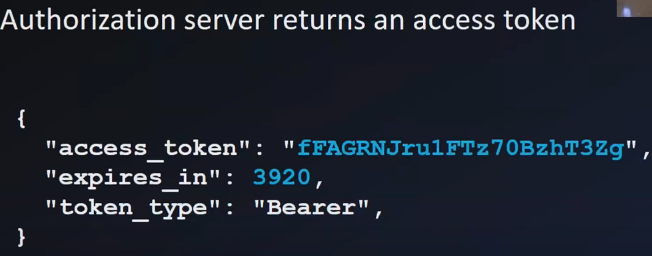
When user provides consent we will get authorization code in the browser address bar, not access token, we will hit again with auth code to get access token and with that we will hit resource server to get contacts



## Procedure to get the access token



Once u got the auth code from the url address bar and hit google api from backend and get the access token,



It has expiration time, as this is valid only for some time and this is valid only for some url like whatever the user have gave the consent if user gave consent to read access to contacts, he can only access them he can’t delete their contacts

When u are completely using front end – react alone or javascript alone then u will directly get the access token in the url I think , because with javascript we may not be able to call backend server to get the access token from the auth code\

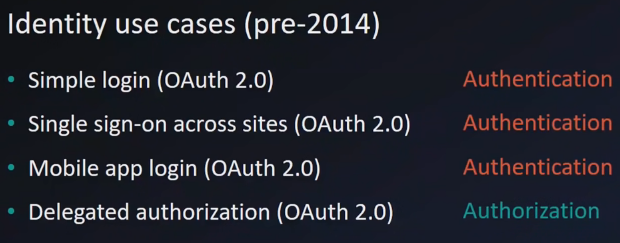
## Use cases of OAUTH

Now auth is used for both authentication and authorization

Like login with facebook , means

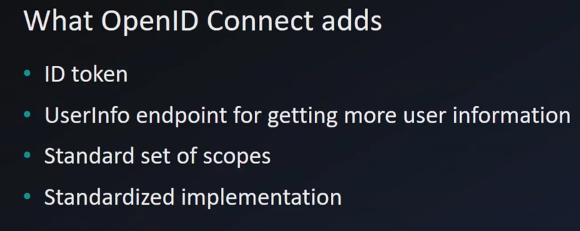
Authorization use case:- to use face book contacts first login and provide the consent and allow access to use contacts

Oauth wasn’t designed to use for authentication, its was designed for authorization only



Now these days they are using open ID connect for authentication and oauth for authorization

OPEN Id connect is just an extension to oauth



If I am talking to an oauth server which can understands open ID connect

I will get access token to talk to resource server and ID token ,,but what s the use of this

And use this access token and hit user info end point and get more details about the use for authorization