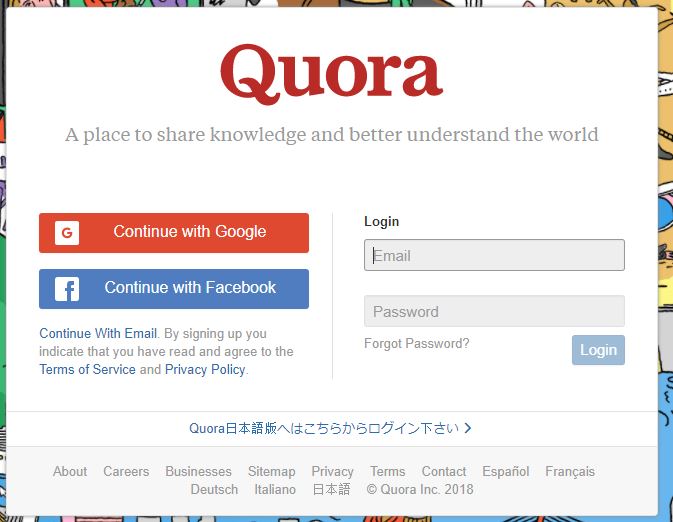
**Spring Boot Security - Introduction to OAuth2**

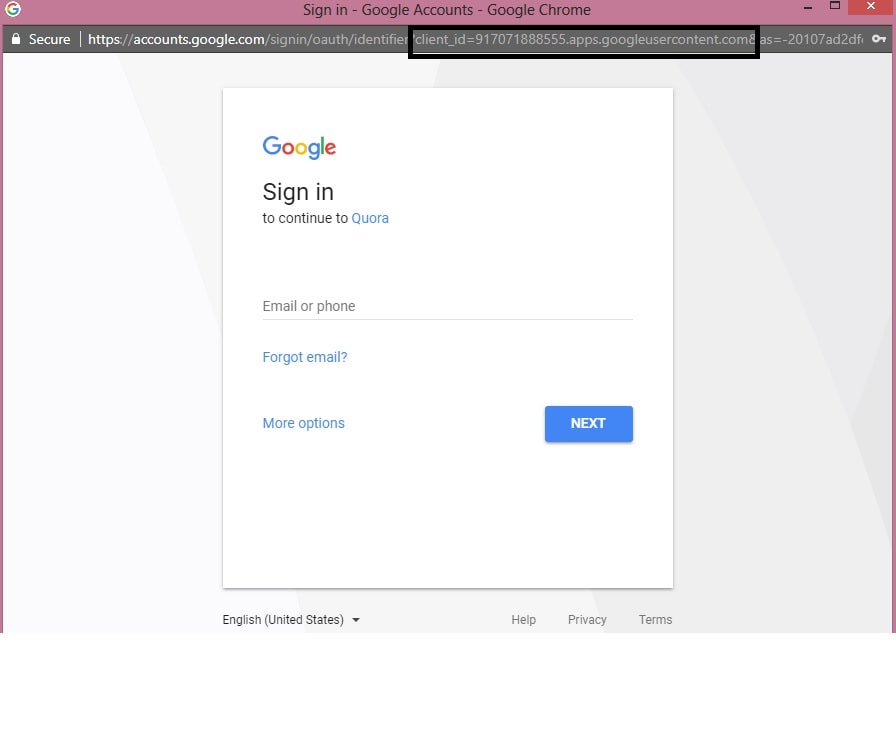
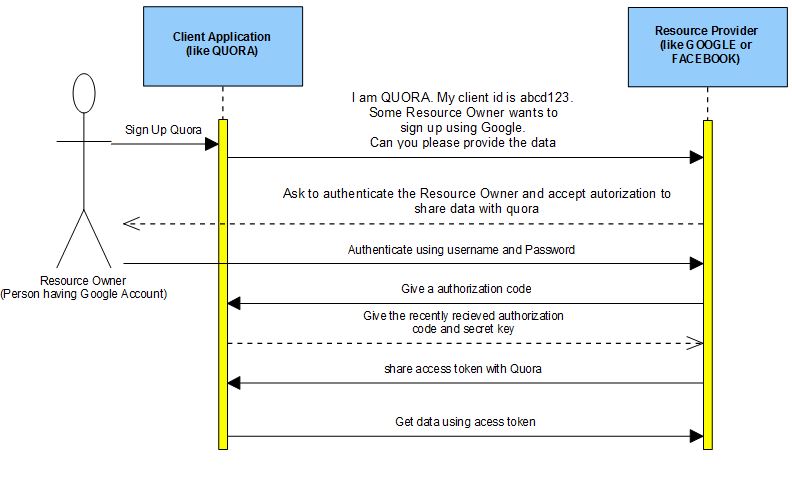
OAuth (Open Authorization) is a simple way to publish and interact with protected data.  
It is an open standard for token-based authentication and authorization on the Internet. It allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password.  
The OAuth specification describes five grants for acquiring an access token:

* Authorization code grant
* Implicit grant
* Resource owner credentials grant
* Client credentials grant
* Refresh token grant

What actually is OAuth?

Consider the use case of Quora. Go to Quora.com.  
If you are a new user you need to signup. You can signup using google or facebook account. When doing so you are authorizing Google or Facebook to allow quora to access you profile info with Quora. **This authorizing is done using OAuth**. Here you have in no way shared your credentials with Quora.  
  
  
In the above example of Quora, we have 3 actors-

* **Resource Owner** - This is the user who wants to sign up using Quora.
* **Client Application** - This will be Quora
* **Resource Server** - This will be Gmail or Facebook.
* **Authorization Server** - The resource server hosts the protected user accounts, and the authorization server verifies the identity of the user then issues access tokens to the application.

In this tutorial we will be implementing our own client application and resource server.  
The **resource owner will then using OAuth authorize the resource server to share data with the client application.**  
The client application must first register with the authorization server associated with the resource server. This is usually a one-time task. Once registered, the registration remains valid, unless the client application registration is revoked. At registration the client application is assigned a client ID and a client secret (password) by the authorization server. The client ID and secret is unique to the client application on that authorization server.  
For example if we click on **Continue with Google**, we get the following screen. Here we can see Quora client id.  
  
Quora got this client id and a secret key when it registered with Google.  
The actual authorization process that takes place between Quora and Google using OAuth is as follows-  
  
Similar to the above flow we will be developing our own client application and Resource Server. Using OAuth the Resource server will then share the data with the client application. Also we will be assuming that the client is already registered with the Resource Server and has been assigned a unique client id and secret key.

* **Spring Boot Client Application** - We already have a unique client id -'javainuse' and secret key - 'secret'. We need to import data from Resource Server.
* **Resource Server** - Using OAuth we configure authorization server. It already has the unique key configured for recognizing our client application.