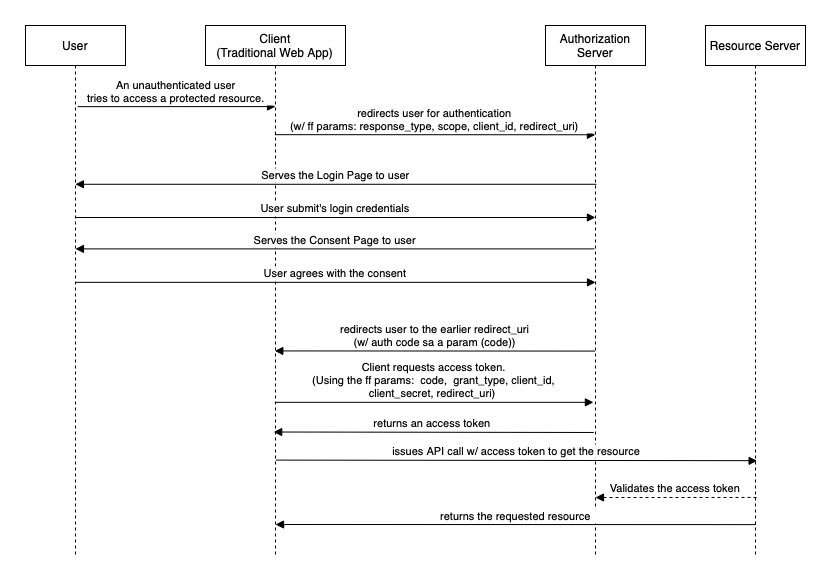
\*\*\* **SSO** stands for Single Sign-On: It's an authentication process that allows a user to access multiple applications or services with a single set of login credentials (such as username and password)

\*\*\* **Oauth2**

OAuth 2.0, in simple terms, is a framework that allows you to grant limited access to your online resources to another application or service, without giving away your password.  
  
Base flow:  
**User** asks for resource -> **Client** redirects to Auth Server -> **Auth** Server provides a login page  
 🡨--------------------- Auth provide a login page ----------------------------|  
 | --------------------- Provide credentials to Auth Server - -----------------🡪  
 <----------------- Redirect to client url - ----------------- |  
 |---------- Client request access token - ----------------->  
 <---------- Auth Server Return Access token ------------|  
 |---------- Call **Resource** server with access token ----------🡪  
 <---------- Validate access token ------------|

Authorization servers often prefer OpenID or Keycloak.

To customize our token and behavior/permission we can override the ‘JwtAuthentication’ token,  
and implements ‘UserDetailService’(assign permissions)  
Overriding the ‘OncePerequest’ filter we manage the authentication process(exceptions, enabled/disabled)