Dynamic Web

Authentication

Authentication

What is authentication?

What purpose does it serve?

How does authentication help us determine what data to get for and from a user?

How does authentication work to determine what data to get?

Authentication Components

Login Form: Submit user data

Authentication Server: A server that checks for valid submitted user data and returns an authentication token

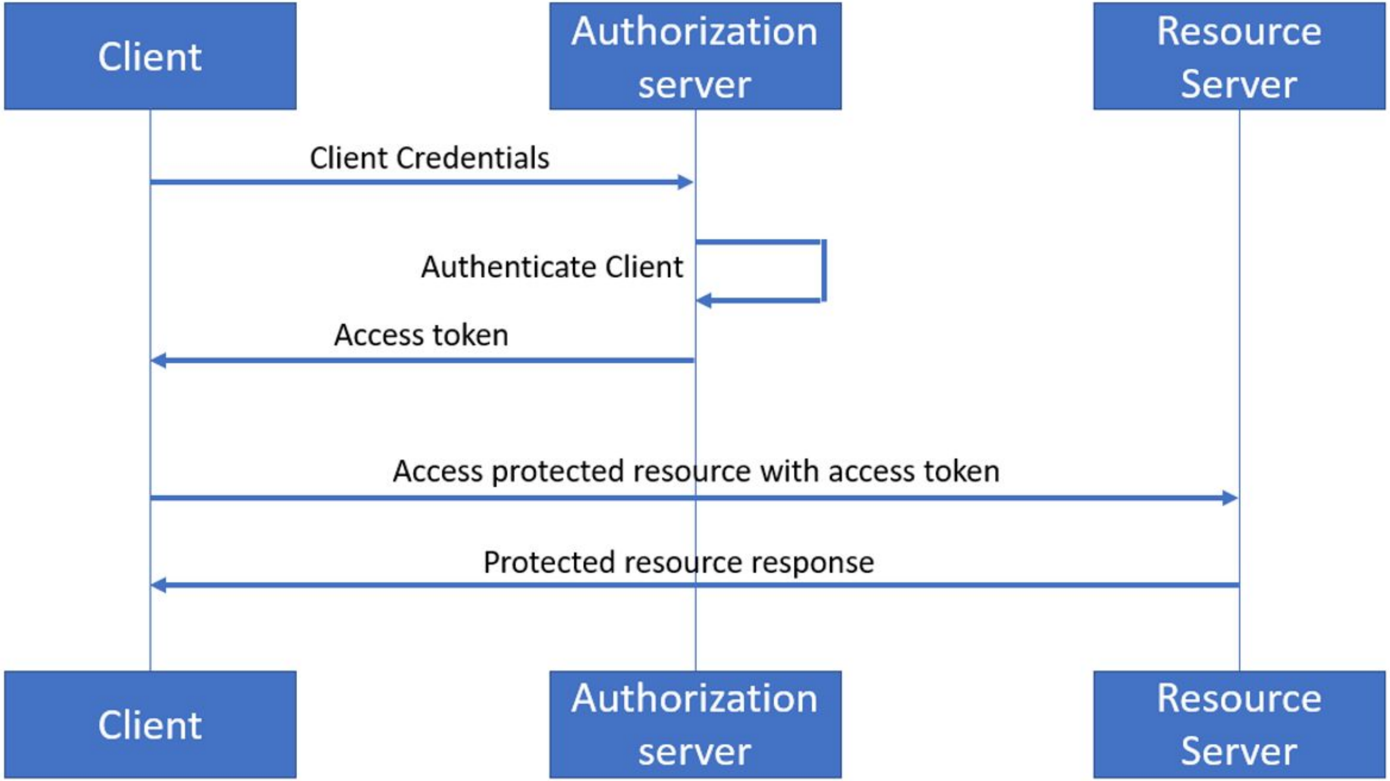
Authentication Token: data that verifies identity

Cookie: Stores auth token and other data to verify identity

Authentication Flow (simplified)

1. User goes to login form
2. User submits (valid) identification credentials
3. Browser sends data (API request) to Authentication Server
4. Authentication Server checks validity of credentials and returns an authentication token
5. Browser will set the auth token as a cookie for future use.
6. User will rely on authentication token for requests to host server

What Auth looks like



How we will be doing Auth

We are going to use **Firebase** for authentication because of its simplicity. This will alter the flow from a more traditional auth flow to letting Firebase control auth.

Take a second to read through the Firebase authentication docs: https://firebase.google.com/docs/auth