Day 21 Spring Security – JWT & Keycloak

Spring Boot Actuator & Metrics of the Running Applications

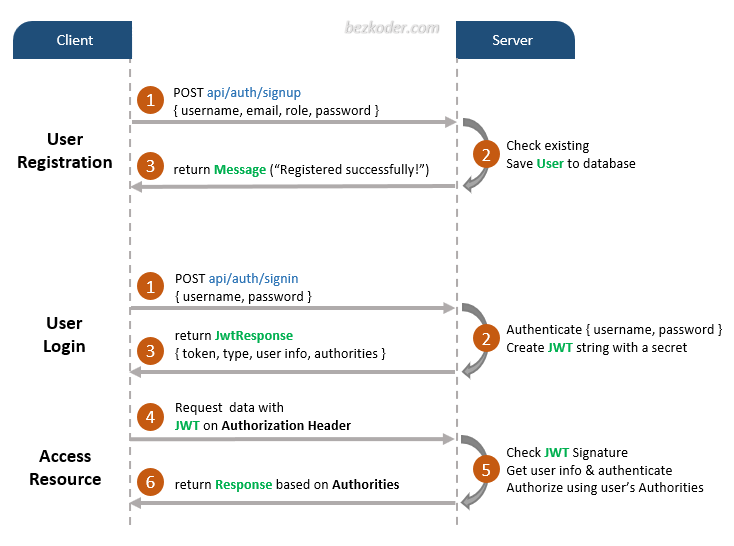
Security – Important Concepts – ARS (Airline Reservation System)

1. Form Based Authentication (Just by adding spring security dependency) – only for Development Environment.
2. Configure Spring Security with the help of DB Tables. (User details needs to be stored in external DB Tables)
3. UserDetails – username, password, authorities (roles) ROLE\_USER, ROLE\_ADMIN (Constant or ENUM)
4. @PreAuthorize, @HasRole,

Token Based Security (JWT based) – Authentication & authorization

JWT – JSON Web Token (Header, PayLoad & Signature [secret-key] )

Bearer (Token) – Request Header (JwtUtil/JwtService)



JWT will be stored in the client side. (Cookies, Session Storage or Local Storage)

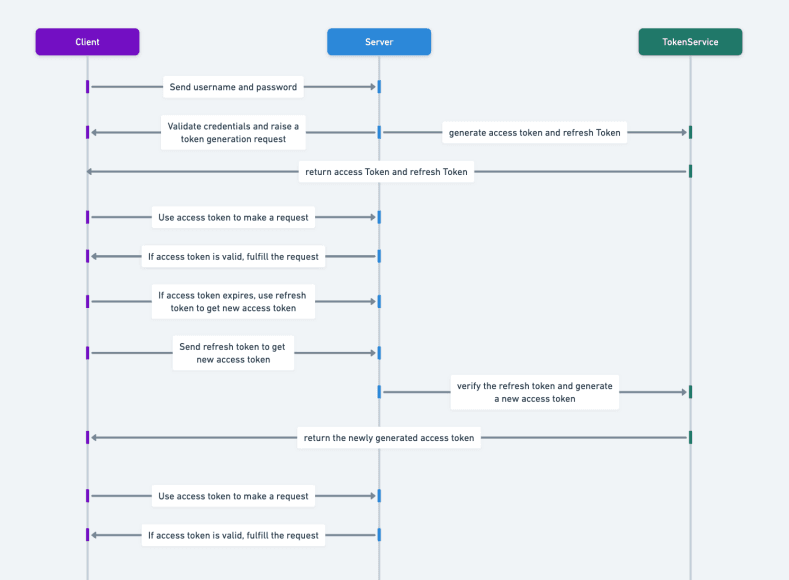
Access Token & Refresh Token.

SpringBoot 3.5.5

JWT 0.11.5

Session will be created after successful authentication (verifying credentials).

sessionId will be there for all the active sessions.



Monolith – Only One Spring Boot Project for the Entire Application. (Mono Repo) – Single Github Repository.

ARS-v2

* User (CRUD on USERS, Forget Password)
* Reservation
* Ratings & Review
* Notification (SMS & Email) –
* Payments
* Airlines
* Security (JWT/OAuth) [Register or Signup, Login or signin, Credentials Expired, User is Inactive, Duplicate Entry – User already registered] (Authenticate & Authorize – RBAC)
* Airports

<https://docs.google.com/spreadsheets/d/1OsjnPBD3x9Zm-YMR69nAA5uiSlPAxAm_HNGhtAv9H9o/edit?gid=0#gid=0>

1. Team Formation (Max 5 Members in a Team)
2. Integrate JWT with our existing ARS application.