Spring Security
Oauth2 + JWT

Jirawong Wongdokpuang

Course Agenda

- Initial Maven Project
  - How to build and run project and project structure

- Start With Basic Spring Security

- Implement Spring Security Oauth2

- Oauth2 Grant Type
  - Resource Owner password credentials
  - Client Credentials
  - Authorization code
  - Implicit

- Enhance Oauth2 with Jwt

Initial Maven Project

- Add first maven dependency

http://projects.spring.io/spring-boot/

Select version 1.3.5.Release

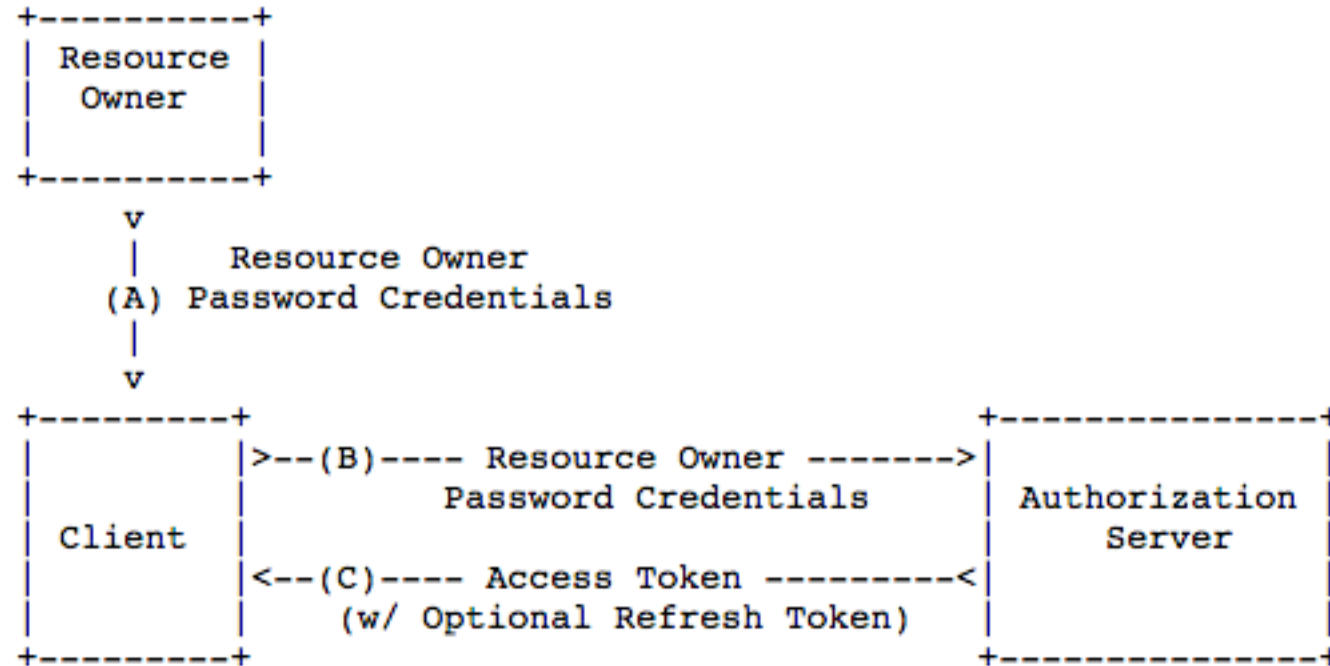# Start With Basic Spring Security

- Add spring-boot-starter-security dependency

- First config with WebSecurityConfig

    - Add inmemory User

Implement Spring Security Oauth2

- spring-security-oauth2 dependency

- ResourceServer

- AuthorizationServer

Oauth2 Grant Type

- Resource Owner password credentials

```
+---------+
| Resource |
|  Owner   |
|          |
+---------+
     v
     |    Resource Owner
 (A) Password Credentials
     |
     v
+--------+                                          +---------------+
|        |>--(B)---- Resource Owner ------->|               |
|        |          Password Credentials    | Authorization |
| Client |                                  |    Server     |
|        |<--(C)---- Access Token ---------<|               |
|        |     (w/ Optional Refresh Token)  |               |
+--------+                                          +---------------+
```

Oauth2 Grant Type

- Client Credentials

```
+---------+                                    +-----------------+
|         |                                    |                 |
|         |>--(A)- Client Authentication --->| Authorization   |
| Client  |                                    |     Server      |
|         |<--(B)---- Access Token ---------<|                 |
|         |                                    |                 |
+---------+                                    +-----------------+
```
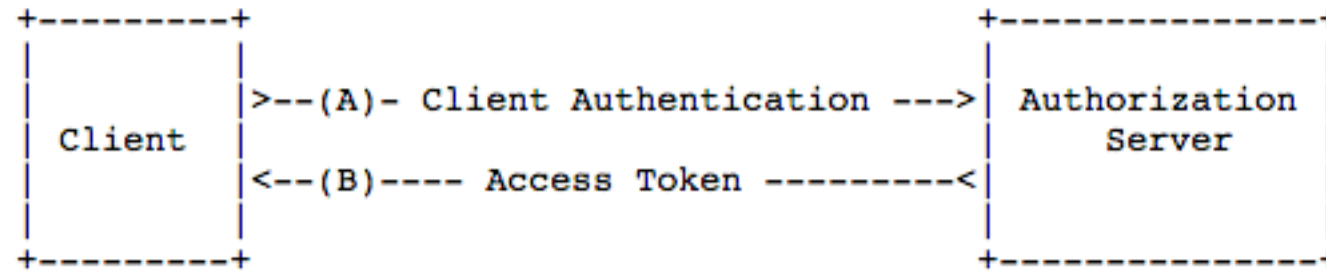
Oauth2 Grant Type

- Authorization code

```
                +---------+
                | Resource |
                |  Owner   |
                |         |
                +---------+
                     ^
                     |
                    (B)
    +----|-----+          Client Identifier          +---------------+
    |          -+----(A)-- & Redirection URI ---->|               |
    |  User-   |                                    | Authorization |
    |  Agent   -+----(B)-- User authenticates --->|    Server     |
    |          |                                    |               |
    |          -+----(C)-- Authorization Code ---<|               |
    +-|----|---+                                    +---------------+
      |    |                                           ^        v
     (A)  (C)                                          |        |
      |    |                                           |        |
      ^    v                                           |        |
    +---------+                                         |        |
    |         |>---(D)-- Authorization Code ---------'        |
    | Client  |          & Redirection URI                    |
    |         |                                               |
    |         |<---(E)----- Access Token --------------------'
    +---------+          (w/ Optional Refresh Token)
```
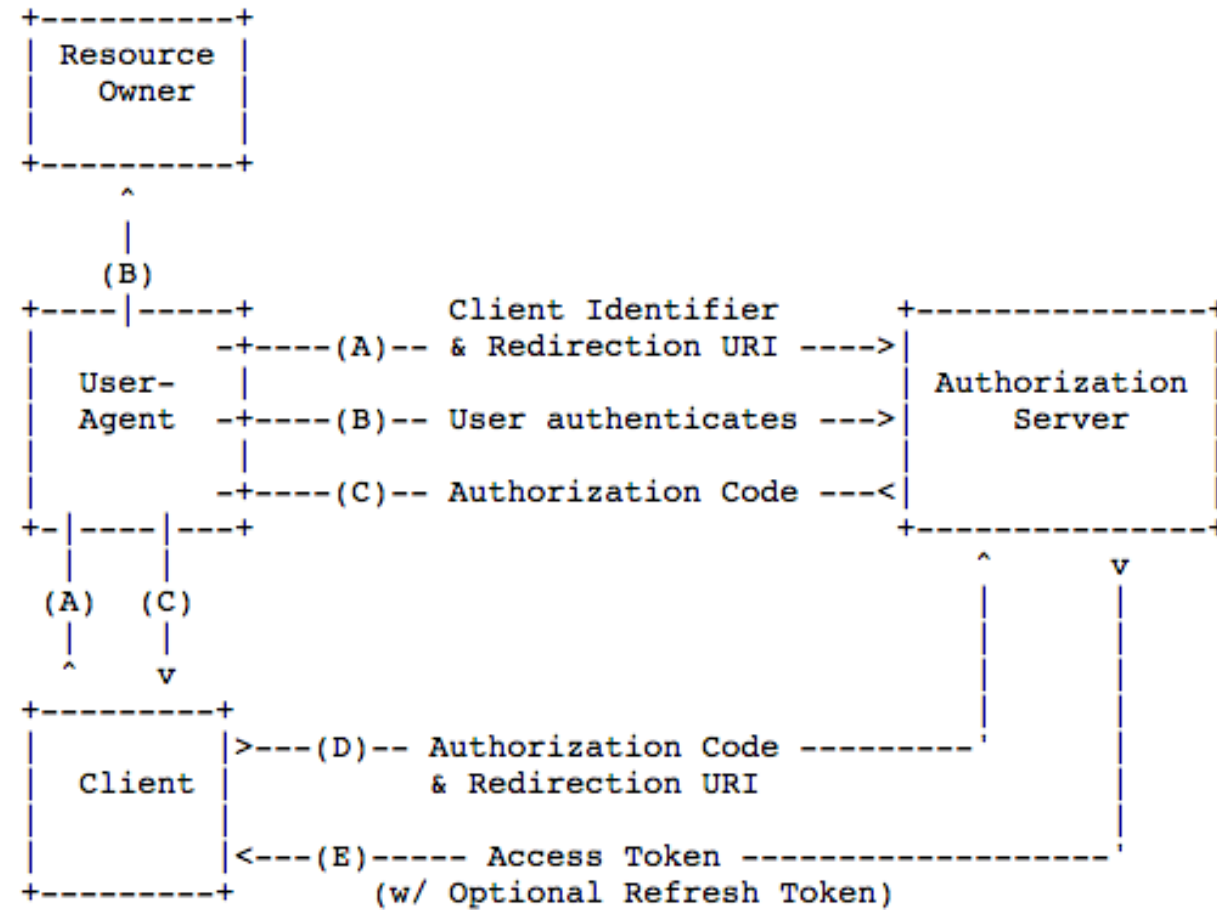
Oauth2 Grant Type

- Implicit

```
                    +----------+
                    | Resource |
                    |  Owner   |
                    |          |
                    +----------+
                         ^
                         |
                        (B)
    +----|-----+          Client Identifier      +---------------+
    |         -+----(A)-- & Redirection URI --->|               |
    |  User-   |                                | Authorization |
    |  Agent  -|----(B)-- User authenticates -->|     Server    |
    |          |                                |               |
    |          |<---(C)--- Redirection URI ----<|               |
    |          |          with Access Token     +---------------+
    |          |            in Fragment
    |          |                                +---------------+
    |          |----(D)--- Redirection URI ---->|   Web-Hosted  |
    |          |          without Fragment      |     Client    |
    |          |                                |    Resource   |
    |    (F)   |<---(E)------- Script --------<|               |
    |          |                                +---------------+
    +-|--------+
      |    |
     (A)  (G) Access Token
      |    |
      ^    v
    +----------+
    |          |
    |  Client  |
    |          |
    +----------+
```
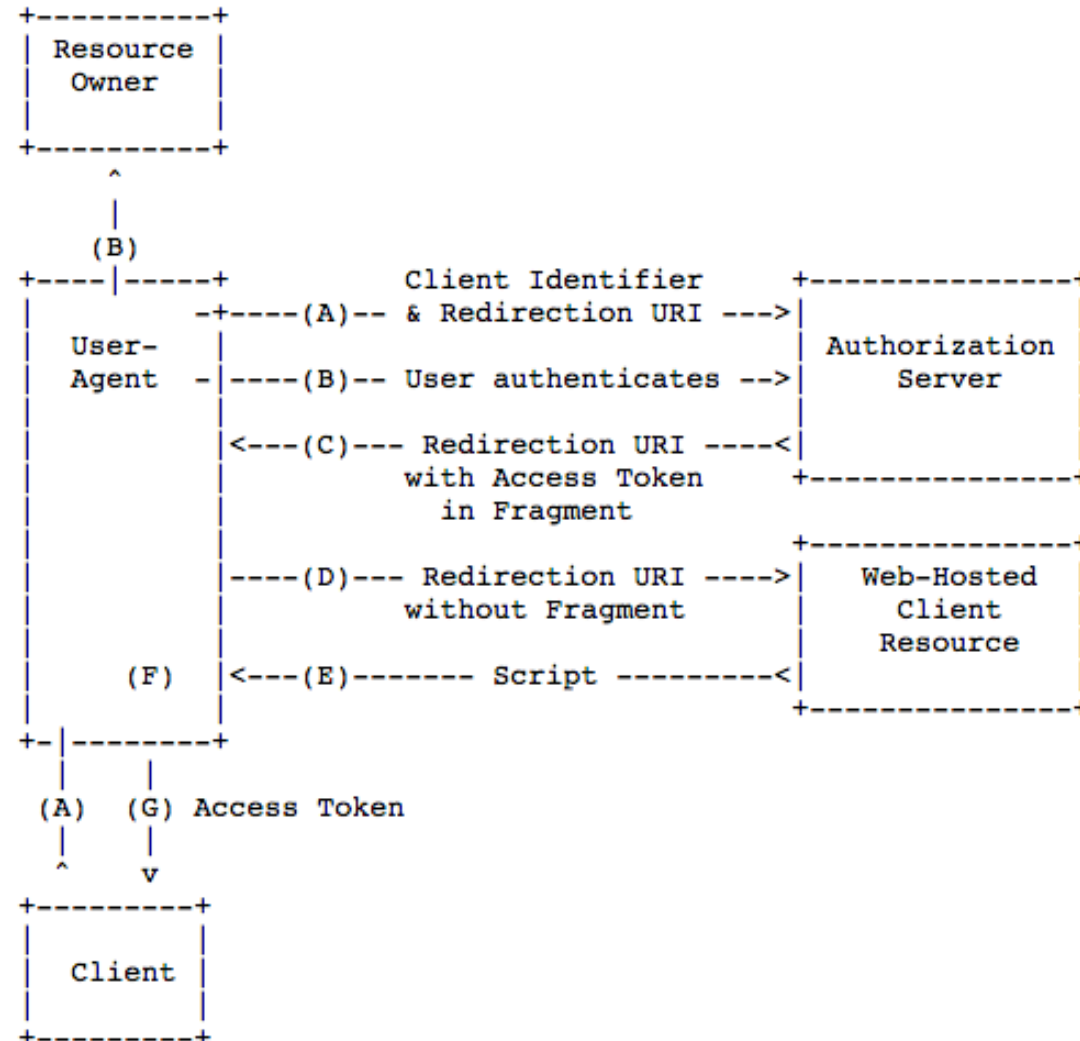
Enhance Oauth2 with Jwt

- Add spring-security-jwt Dependency

- Implement AccessTokenConverter

- Improve Jwt Imformations with enhance method

Q & A