IMPLEMENT : AUTH

1. INSTALL + SETUP : IDENTITY FRAMEWORK
2. DB WORK - MIGRATION
3. USER SERVICE
4. USER CONTROLLER
5. DTO's - LOGIN, REGISTER, USER

- REGISTER() — USERNAME, PASSWORD, NAME, EMAIL — DTO
- LOGIN() /API/LOGIN — USERNAME, PASSWORD — DTO
- 3

{ USER : JOHN
EM: ...
3

AUTHENTICATE

1 REGISTER

POST /API/USERS/REGISTER

USERS CONTROLLER

{ USERNAME PASSWORD EMAIL }

RegisterUserDto

- HANDLE REG-L FIELDS
- TRANSFER FROM CLIENT → SERVER
- SHAPES DATA
- CONTRACT ✓

DTO {}

"USERSERVICE"

Register (DTO)

IDENTITY CREATE !

SUCCESS - DTO

FAIL - ERRORS

DTO or NULL

BACK TO CONTROLLER {DTO?}

↓

CLIENT

2 LOGIN (AUTHENTICATION)

AUTHORIZATION

PERMISSIONS — WHAT CAN YOU DO?

CLAIM

1. WHAT KIND OF USER ARE YOU?
   GROUPS, ROLES - EDITOR, ADMIN, WRITER, GUEST

POLICY

2. WHAT ACTUAL PERMISSIONS DO YOU HAVE?
   READ, CREATE, FILM, AND MUSIC

ROUTE

GET /ME

* [AUTHORIZE (POLICY = "EAT")]

PUBLIC XYZ ( ) {

PRINT

}

ROUTE PROTECTION

TOKEN

"you"

JSON WEB TOKEN (JWT)

"JAWT"

DATA

1. REGISTER
2. LOGIN

> USERDTO
> - USERNAME
> - ID
> - ★ TOKEN (JWT) ← IS YOUR CLAIM

---

3. VISIT A ROUTE w/ [AUTHORIZE] ...

TOKEN TO BE SENT

① IS TOKEN VALID? ✓
② WHO IS THIS USER? ✓
③ WHAT ARE PERMISSIONS? ← IDK [ANNOTATION]

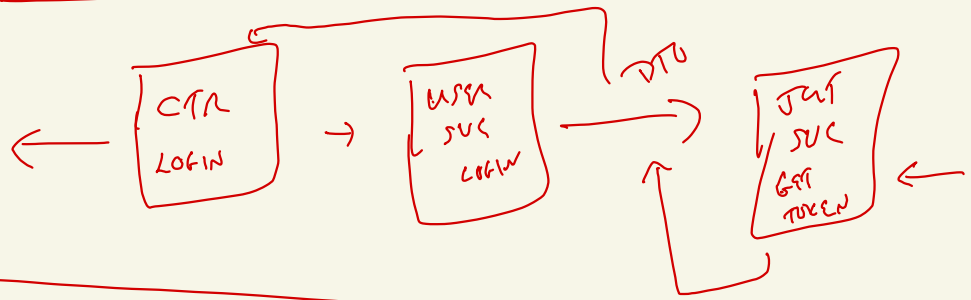
① LOGIN (API)

↳ USER SERVICE . LOGIN (u, p)

↳ IDENTITY (USER MANAGER)

USER → GETTOKEN

RETURN DTO ← USERID, TOKEN



② [AUTHORIZE]

[HTTP GET]

JWT SERVICE. AUTHORIZE

READS TOKEN FROM REQUEST (HEADER)

VALIDATE (BODY) ← USER

ERR