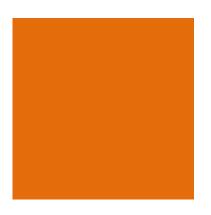
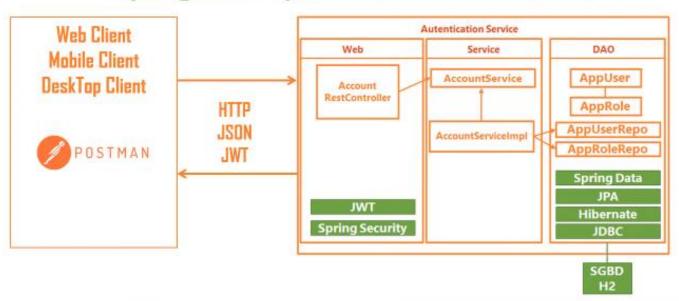
**JWT** 



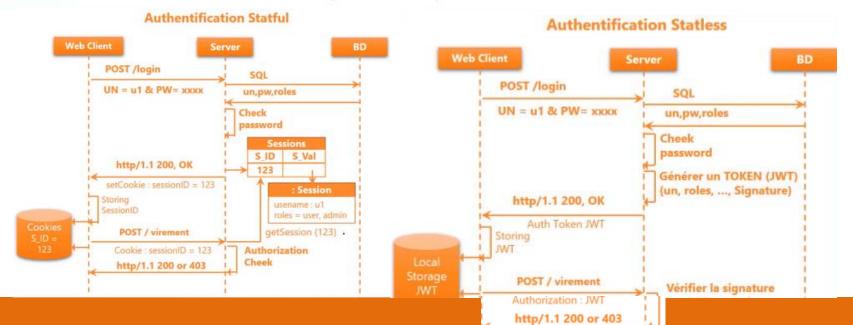


### Authentification Stateless avec Spring Security et Json Web Token (JWT)



### Systèmes d'authentification

- Deux types de modèles d'authentification :
- Statful: Les données de la session sont enregistrés coté serveur d'authentification
- Statless: les données de la session sont enregistrés dans un jeton d'authentification délivré au client.



### Json Web Token (JWT)

- JSON Web Token (JWT) est un standard (RFC 7519) qui définit une solution compacte et autonome pour transmettre de manière sécurisée des informations entre les applications en tant qu'objet structuré au format JSON (Java Script Object Notation).
  - Compact: en raison de leur petite taille, les JWT peuvent être envoyés via une URL, un paramètre POST ou dans un en-tête HTTP. De plus, la plus petite taille signifie que la transmission est rapide.
  - Autonome: Le JWT contient toutes les informations requises sur l'utilisateur, ce qui évite d'avoir à interroger la base de données plus d'une fois pour connaître le détail de l'identité d'un client authentifié.
- Le JWT est fiable car il est signé numériquement.
- JWT est constitué de trois parties séparées par un point « . » :
  - Header
  - · Payload
  - Signature

La forme d'un JWT est donc :

eyJmeGc1GiJTuzlTW11mInR5cC16IxpxvCJP.eyJ zd811011x9yMMRTV300xzl1eiaXdz1jnia#86c0 vL2xvY2FasGPzdG-4MCgeL2F1dSqiLCJmdW10101 1VZV31E2yd25dTEVa2ClnfX1vvvls2Sd86cA4xXm iJXhm1jn1MGc40TAxMDejbmJn1jpud8xxlCJyVXQ 10j050GV1MCMytCJgdfX1DijDzN1MyJUMZZ8cd1g MPGx4MZY1LCJvWXV1TjpiNWVLixice9xZXXfxDln 1VMRx4M31LCJvXXV1TjpiNWVLixice9xZXXfxDln 1VMRx4M31LCJmXXMDSTLXXXX.

V4FXAPplBx1HqCMUSqp7ptqzqXZRrolDlhj4cVAQ V0

xxx.yyy.zzz

```
Header
```

```
{
    "alg": "HS256",
    "typ": "JWT"
}
```

Encodage Base 64 URL

eyJhbGciOiJIUzI1NilsInR5cCl6lkpXVCJ9

### Payload

```
{
    "sub": "1234567890",
    "iss":"http://localhost:8080/auth",
    "aud":["Web Front End","Mobile App"],
    "exp":54789005,
    "nbf":null,
    "iat":49865432,
    "jti":"idr56543ftu8909876",
    "name": "med",
    "roles":["admin","author"]
}
```

Encodage Base 64 URL

eyJzdWliOilxMjM0NTY3ODk wliwiaXNzljoiQmFja2VuZClsl mF1ZCl6WyJXZWlg .... vciJdfQ

Signature : RSA ( 2 clés publiques et privée ) ou HMAC (1 clé privée)

HMACSHA256( base64UrlEncode(header) + "." + base64UrlEncode(payload), secret)

V4FXAPplBx1HqONU6qp7ptqzq32RrolDlhj4cVUQV0

#### Encoded

eyJBeXA101JKV1Q1LCJhbGc101JIUzUxW1J9.e
yJpc3M101I1LCJpYXQ10jE2Mzg5NzM8MTYsImV
4cC16MTY3MDUw0TQxNyw1YXVkIjo1Iiw1c3V1I
jo1YWRtaW41LCJSb2x1IjpbIk1hbmFnZXI1LCJ
BZG1pb1JdfQ.haE7cPUhsCPWJHvd5IJpqnyI8H5c9Y35vhkLDrMM8WjwRZs5zuI7PzKim1sQa
nK7f5tIXfZL12VTSxnY2\_epA

#### Decoded

```
HEADER ALCOHOMA TOWN TYPE
   CIVE COUNTY
   "mig": "Hosta"
FWILDAM DESK
    "Lat" - 1628973416.
    "wyp": 1679509477.
    Capable 11
    "sidn" "aded n"...
    'Role |
     "Hanager".
     CARREAC
VEREY SIGNATURE
  basepAvrlEncode(needer) + "." +
  beset-furlEncode(payless).
  S secret basel4 secoded
```

Signature Verified

SHARE JWT