

Bonus: JWT



Goal

JSON Web Tokens

- authorization
- exchange of data

Not Akka HTTP specific, but often used in web apps/microservices



JWT Authorization

Principles

- you authenticate to the server (username + pass, OAuth, your blood etc)
- server sends you back a string aka token
- you then use that string for secure endpoints
 - special HTTP header Authorization: (token)
 - the endpoint will check the token for permissions
 - your call is allowed/rejected

Result: authorization

- not authentication: you receive the token after authenticating

JWT Structure

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyb2NrdGh1anZtLmNvbSIsImV4cCI6MTU2MDgxOTM4MCwibmFtZSI6IkrHbmllbCBDaW9jaXJsYW4iLCJhZG1pbI6dHJ1ZX0.x1YLh0enJkRE6iI4Syf6TuHqYze_HjLYtw49yyjp8Q
```

Part 1: header

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

Base64 encode

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

header JSON:

- type = JWT
- hashing algorithm = HMAC SHA256

JWT Structure

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyb2NrdGhlanZtLmNvbSIsImV4cCI6MTU2MDgxOTM4MCwibmFtZSI6IkJhbmllbCBDaW9jaXJsYW4iLCJhZG1pbSI6dHJ1ZX0.x1YLh0enJkRE6iI4Syf6TuHqYze_HjLYtw49yyjp8Q
```

Part 2: payload (claims)

```
{  
  "iss": "rockthejvm.com",  
  "exp": 1300819380,  
  "name": "Daniel Ciocirlan",  
  "admin": true  
}
```

Base64 encode

```
eyJpc3MiOiJyb2NrdGhlanZtLmNvbSIsImV4cCI6MTU2MDgxOTM4MCwibmFtZSI6IkJhbmllbCBDaW9jaXJsYW4iLCJhZG1pbSI6dHJ1ZX0
```

Registered claims (standard)

- issuer
- expiration date

Public claims (custom)

- name
- admin
- any kind of permissions

JWT Structure

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyb2NrdGhlanZtLmNvbSI6ImV4cCI6MTU2MDgxOTM4MCwibmFtZSI6IkJhbm1lbCBDaW9jaXJsYW4iLCJhZG1pbSI6dHJ1ZX0.x1YLh0enJkRE6iI4Syf6TuHqYze_HjLYtw49yyjp8Q
```

Part 3: signature

- take encoded header + "." + encoded claims
- sign with the algorithm in the header and a secret key
- encode base64

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyb2NrdGhlanZtLmNvbSI6ImV4cCI6MTU2MDgxOTM4MCwibmFtZSI6IkJhbm1lbCBDaW9jaXJsYW4iLCJhZG1pbSI6dHJ1ZX0
```

HS256 (secretKey)

```
QWV_bzJ2waQfNZE_OsdXPdC7TCQqVv1eREv95icLcxA
```

```
QWV_bzJ2waQfNZE_OsdXPdC7TCQqVv1eREv95icLcxA
```

Base64 encode

```
x1YLh0enJkRE6iI4Syf6TuHqYze_HjLYtw49yyjp8Q
```

Akka rocks

