**JWT Token Authentication**

JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the **HMAC** algorithm) or a public/private key pair using **RSA** or **ECDSA**.

**Format of JWT Token:**

* Header
* Payload
* Signature

**Header:**

Header contains the Token type and the signing algorithm used for signing credentials(Key).

**Payload:**

Payload contains the claims that can be registered claim or custom claim. Here claims are considered as entity to hold the information which needs to be transmitted to the other party/Api.

Example of Registered claims are: **iss** (issuer), **exp** (expiration time), **sub** (subject), **aud**(audience)

**Issuer:** The API in which the token is generated

**Audience**: The Recipients of the token

The Header and payload are **Base64Url** encoded to form the second part of the JSON Web Token.

Example:

var authSigningKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes("SecureKeyRequiredforvalidationAdmin"));

var authClaims = new[]

{

new Claim("UserName", UserName),

new Claim("Role", Role)

};

var token = new JwtSecurityToken(

issuer: "https://localhost:44316",

audience: "https://localhost:44393/GatewayAPI",

expires: DateTime.Now.AddDays(1),

claims: authClaims,

signingCredentials: new Microsoft.IdentityModel.Tokens.SigningCredentials(authSigningKey, SecurityAlgorithms.HmacSha256)

);

Signature:

The signature part will be created with the encoded header, the encoded payload, a secret, the algorithm specified in the header, and signed with the signing credentials.

HMACSHA256(

base64UrlEncode (header) + "." +

base64UrlEncode(payload),



)

**Encoded token:**

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVc2VyTmFtZSI6IkplZmYiLCJSb2xlIjoiQWRtaW4iLCJleHAiOjE2MDEwNjMwNDMsImlzcyI6IkFXVFVzZXIiLCJhdWQiOiJBV1RVc2VyIn0.i1O-ngwYej7gU0f7bPAkXepJWu5Sw1KVFvDflcddFXI

**Header:**

{

"alg": "HS256",

"typ": "JWT"

}

**Payload:**

{

"UserName": "Jeff",

"Role": "Admin",

"exp": 1601063043,

"iss": "AWTUser",

"aud": "AWTUser"

}