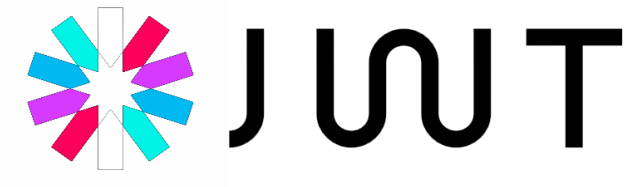

JSON Web Tokens

JWT is an open standard (RFC 7519) for securely transmitting information between parties as a JSON object. It is compact, self-contained, and used widely in authentication and information exchange scenarios. JWTs are digitally signed, ensuring the data integrity and authenticity of the message.

JWT Structure

JWT consists of **three parts**, separated by dots (`.`):

1. Header

- Contains metadata about the token.
- Typically includes:
  - ❖ The type of token (JWT).
  - ❖ The signing algorithm used (e.g., HS256, RS256).

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

2. Payload

- Contains the claims, or the data to be transmitted.
- Claims can be:
  - ❖ **Registered claims**: Predefined claims like iss (issuer), exp (expiration time), sub (subject), and aud (audience).
  - ❖ **Public claims**: Custom claims that are agreed upon between parties.
  - ❖ **Private claims**: Custom claims used within an organization.

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

3. Signature

- Ensures that the token has not been altered.
- Created by encoding the header and payload, then signing it with a secret key or private key.

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

JWT Authentication Flow