JSON Web Tokens JWT

JWT stands for JSON WEB TOKENS , JWT is an open industry standard (RFC 7519) used to share information between two entities, in my case as a back-end developer usually a client (website's frontend) and a server (website's backend).

A token is a secure string representing data, like user details or permissions, used for authentication and verification.

We use tokens and not plain JSON because plain JSON cannot ensure data integrity or security during transmission, as it can be easily tampered with by attackers. Tokens, such as JWTs, address this by including a secure signature that allows the client to verify the authenticity of the data .

It contains JSON objects which have the information that needs to be shared. Each JWT is also signed using cryptography to ensure that the JSON contents (also known as JWT claims) cannot be altered by the client or a malicious party.

A JWT has three parts:

1. **Header**: Specifies the token type (JWT) and signing algorithm.
2. **Payload**: Contains the claims or data.
3. **Signature**: Ensures the payload's integrity using a cryptographic algorithm.

This is how JWT works

1. When a user logs in, the server generates a JWT containing the user's data and an expiration time.

2. The token is signed with a secret key and sent to the client.

3. For the following requests, the client includes the JWT in the request header.

4. The server then verifies the token's integrity and checks its validity before processing the request.

We use JWT for secure, stateless authentication. It enables secure transmission of user data without storing session data on the server, enhancing security in systems.