

JSON Web Token (JWT)

Justin Katerberg, Ammar Khan, Connor Henderson

What It Is

- Open standard that defines a compact and contained method to securely transmit information as a JSON object
- Information that is transmitted is digitally signed
- Contains 3 parts
 - Header
 - Gives information about itself, such as what it is and what type of algorithm is used
 - Payload
 - Actual data carried by token
 - Signature
 - Sum of encoded header and encoded payload. Provides error/tamper checking
- Final encoded JWT looks as follows, notice the periods separating the sections

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImRlc3QiLCJ1c2VySWQiOiJiZW
MwZTYxOC0xYjg1LTQwZjEtYmRlZC0zZGY5ZGE3MTk2MTEiLCJpYXQiOiE2MTg3MDI2MzY
slmV4cCI6MTYxODc0OTAzNn0.Q14EvQgVHTY3_zV2_dkoKgEjM7yC_GDjOLCPn4Ld3mY

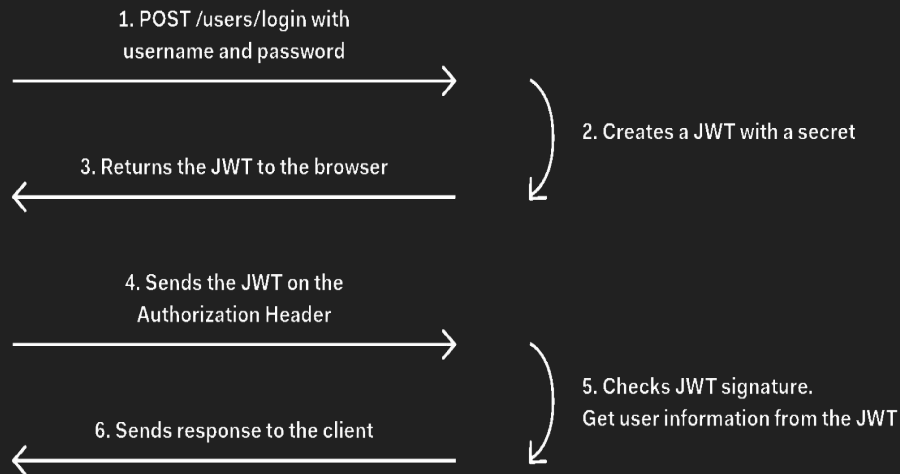
Use Case

- Client Authorization

- JWT is issued to client
- Client sends JWT back to server along with every request
- Server checks JWT, verifies that user is authorized to make the request
- Server responds

Browser

Server



Usage (Node)

- Using jsonwebtoken (npm)

```
1 //import library
2 var jwt = require('jsonwebtoken')
3
4 //Secret key, used to encrypt token
5 let secret = "This could be anything, not recommended to store it in version control";
6
7 //data to send in the key
8 let data = {
9   user_id: id_for_user,
10  other_stuff: anything_else_to_store
11 }
12
13 //some optional parameters for the token. See https://www.npmjs.com/package/jsonwebtoken
14 //for all options
15 var options = {
16   algorithm: 'HS256', //Algorithm to use for encryption
17   expiresIn: '24h', //Set how long the token is valid for
18   notBefore: '1h', //Set when token should become valid
19 }
20
21 //Generating a token. This can be sent to the client for use in future authentication
22 let token = jwt.sign(data, secret, options);
23
24 //Verifying validity of token, boolean
25 const verified = jwt.verify(token, secret);
```

References

How JWT works - in depth. *Cambrose, A.* 2020/06/04. <https://medium.com/swlh/how-jwt-works-in-depth-604c93ec20a4>

Introduction to JSON Web Tokens. <https://jwt.io/introduction/>

JSON Web Token (JWT). <https://tools.ietf.org/html/rfc7519>

JSON web token | JWT. 2019/03/28. <https://www.geeksforgeeks.org/json-web-token-jwt/>

jsonwebtoken. <https://www.npmjs.com/package/jsonwebtoken>

Build Secure (JWT) Token Based Authentication API with Node. *Digamber.* 2021/03/31.
<https://www.positronx.io/build-secure-jwt-token-based-authentication-api-with-node/>