JWT

JSON WEB Token

JWT is pronounced as “jot”

JWT

securely transmits information between two parties

Why do we use JWT?

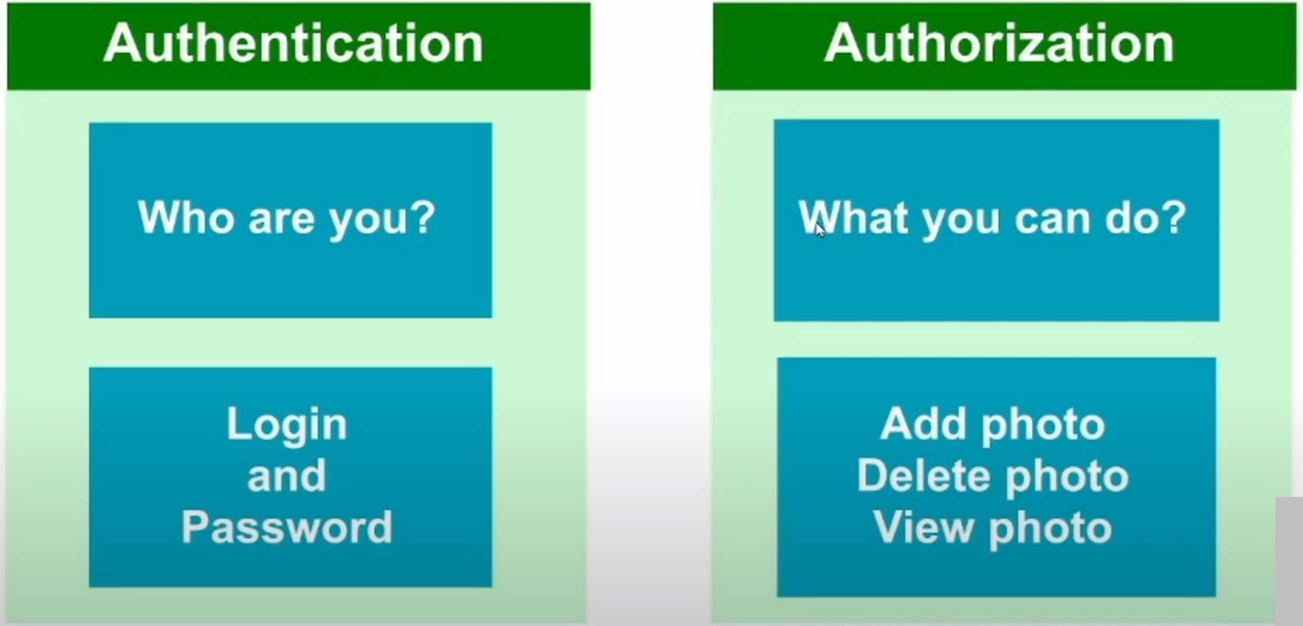
Without JWT you can access the protected route

http://local:5000/orders?email=abc@gmail.com
H
confidential data

With JWT you can't access the protected route

http://local:5000/orders?email=abc@gmail.com
H
"messsage":" User not authorized"

JWT is mainly used for authorization purpose, not authentication



Authentication

Who are you?

Login
and
Password

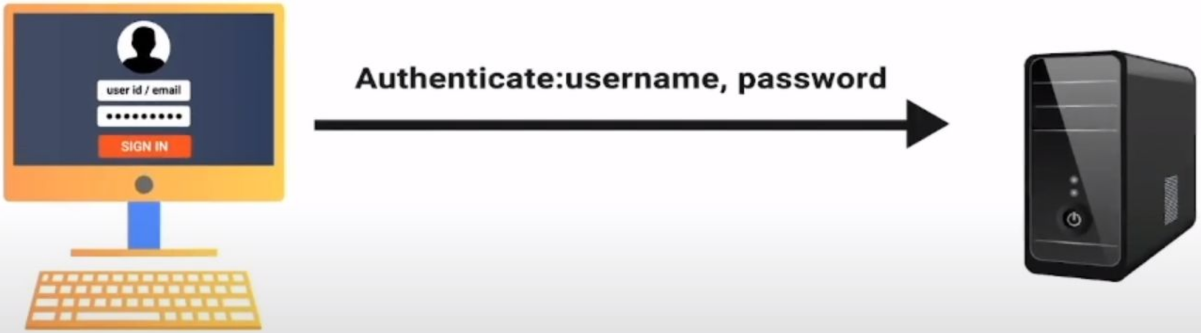
Authorization

What you can do?

Add photo
Delete photo
View photo

HOW JWT WORKS?

1. Client login with username and password



Authenticate:username, password

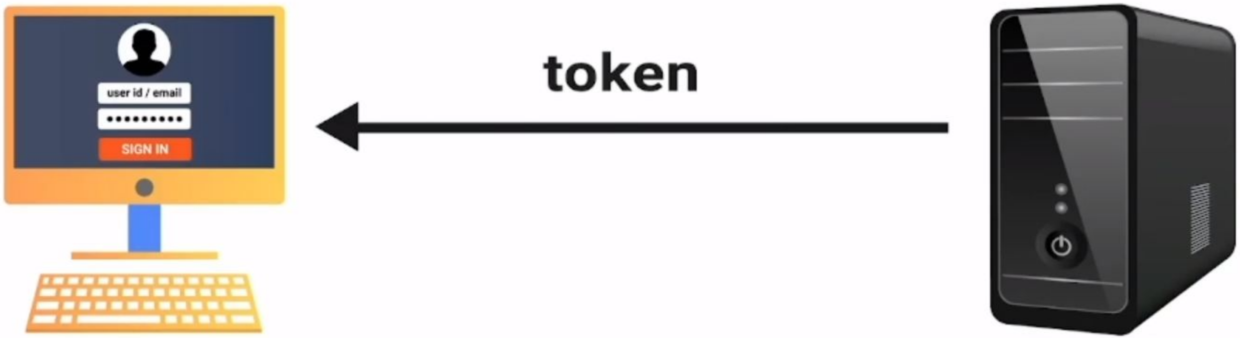
HOW JWT WORKS?

2. Server creates a token for the client

user id / email
SIGN IN
JWT

HOW JWT WORKS?

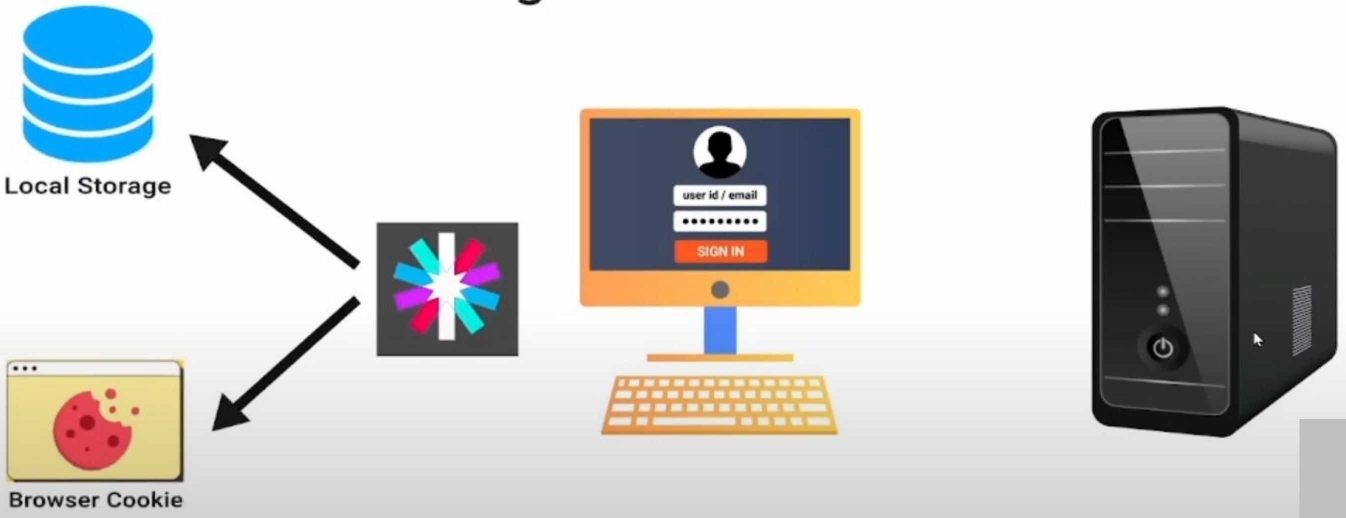
3. server sends a token to the client



token

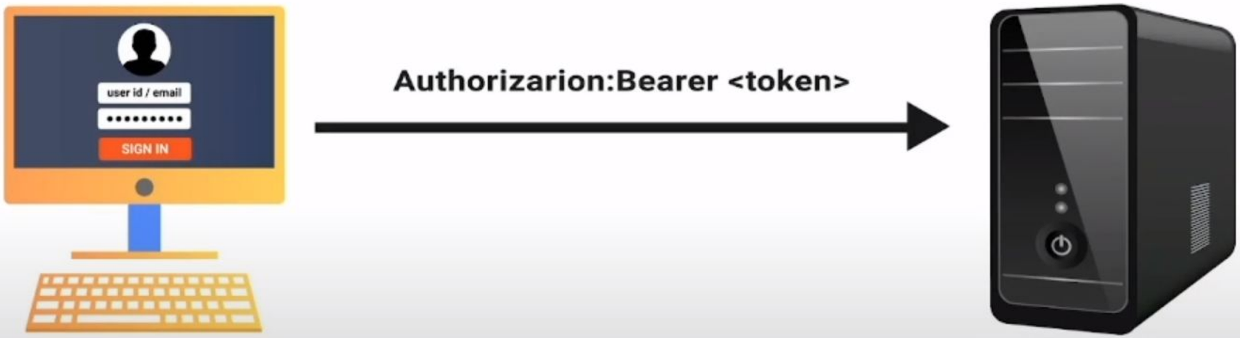
HOW JWT WORKS?

4. Client stores the token on either local storage or browser cookie



HOW JWT WORKS?

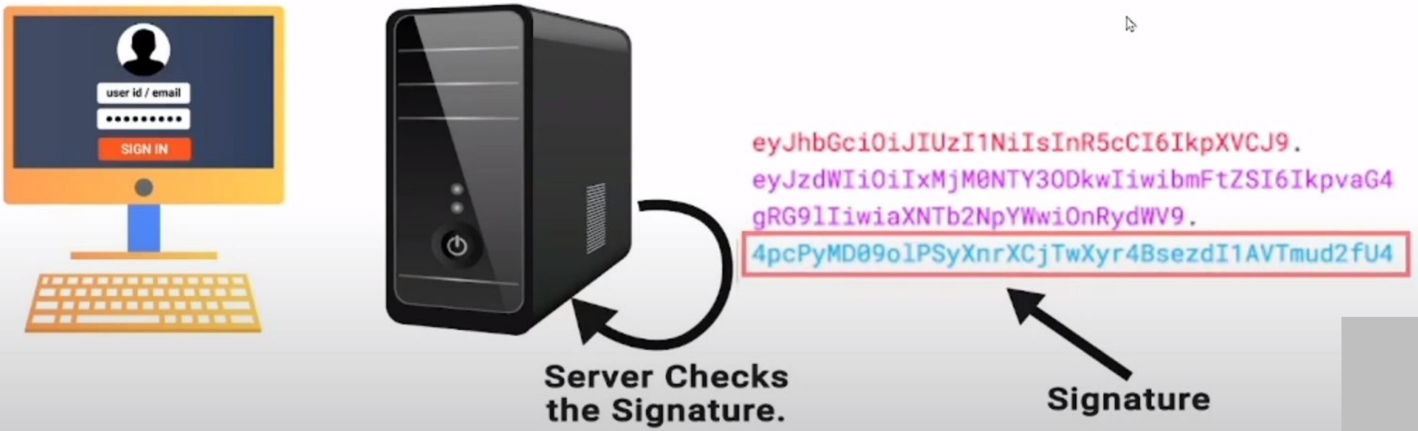
5. Next time the client makes a request, a copy of the token is send to the server for authorization.



Authorizarion:Bearer <token>

HOW JWT WORKS?

6. Server verifies the JWT signature before giving the authorization.



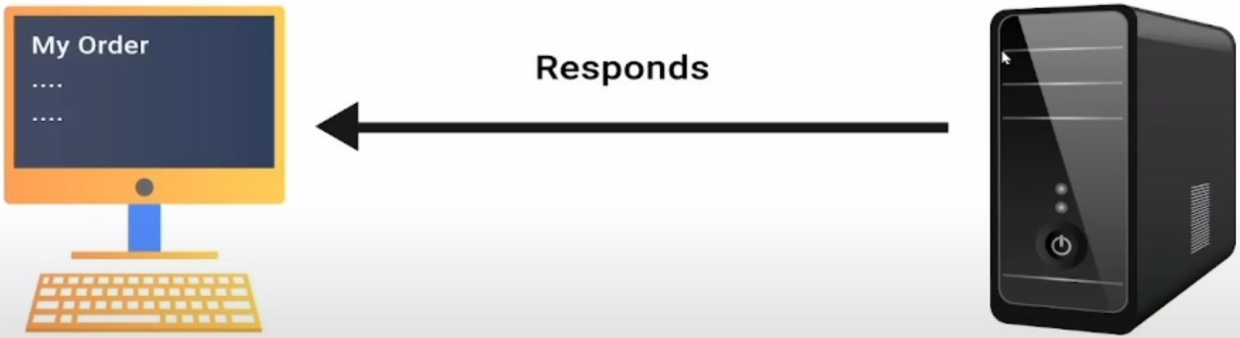
```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

Server Checks the Signature.

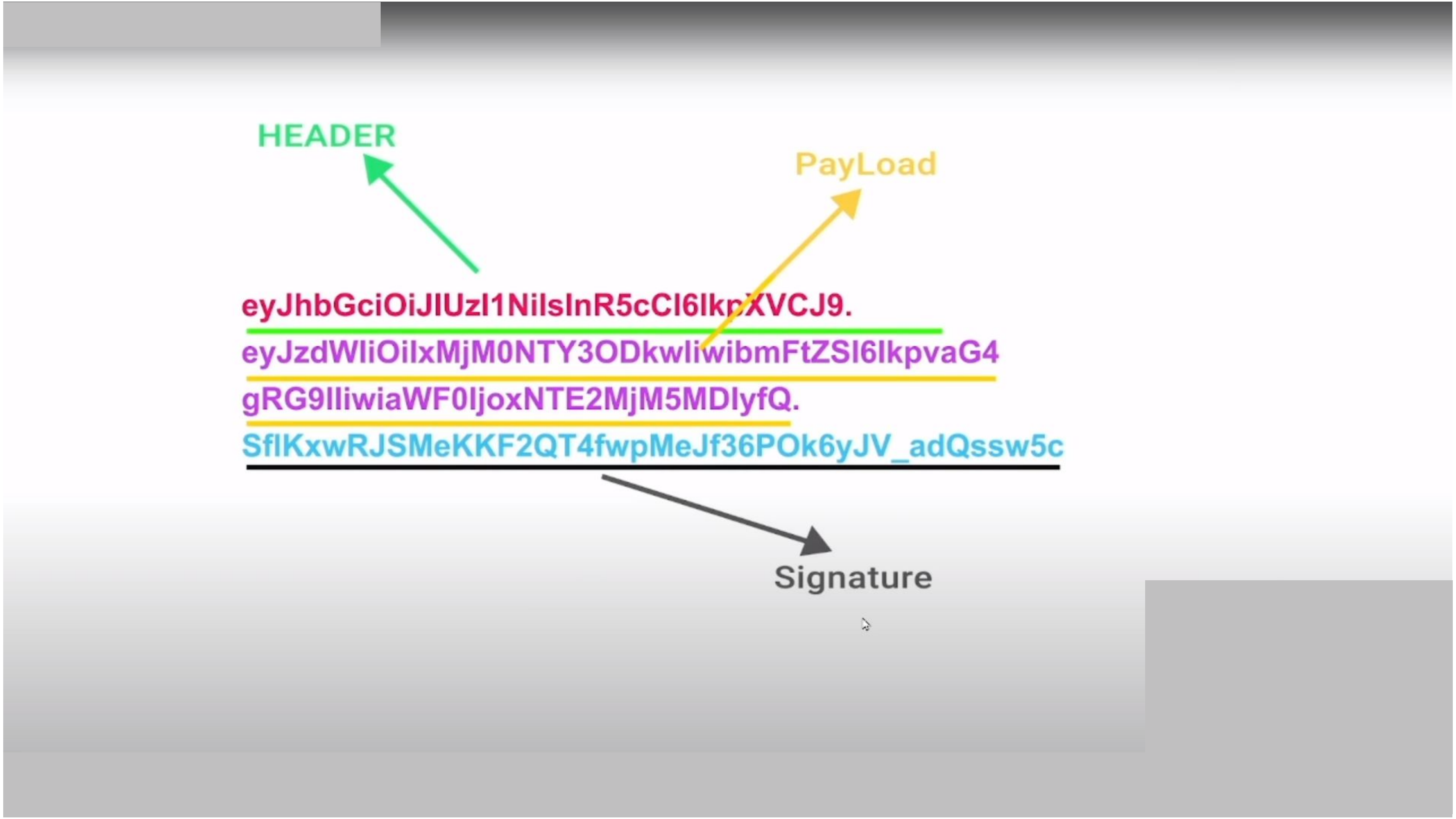
Signature

HOW JWT WORKS?

7. Server responds to the client's request.



WHAT JWT LOOKS LIKE?



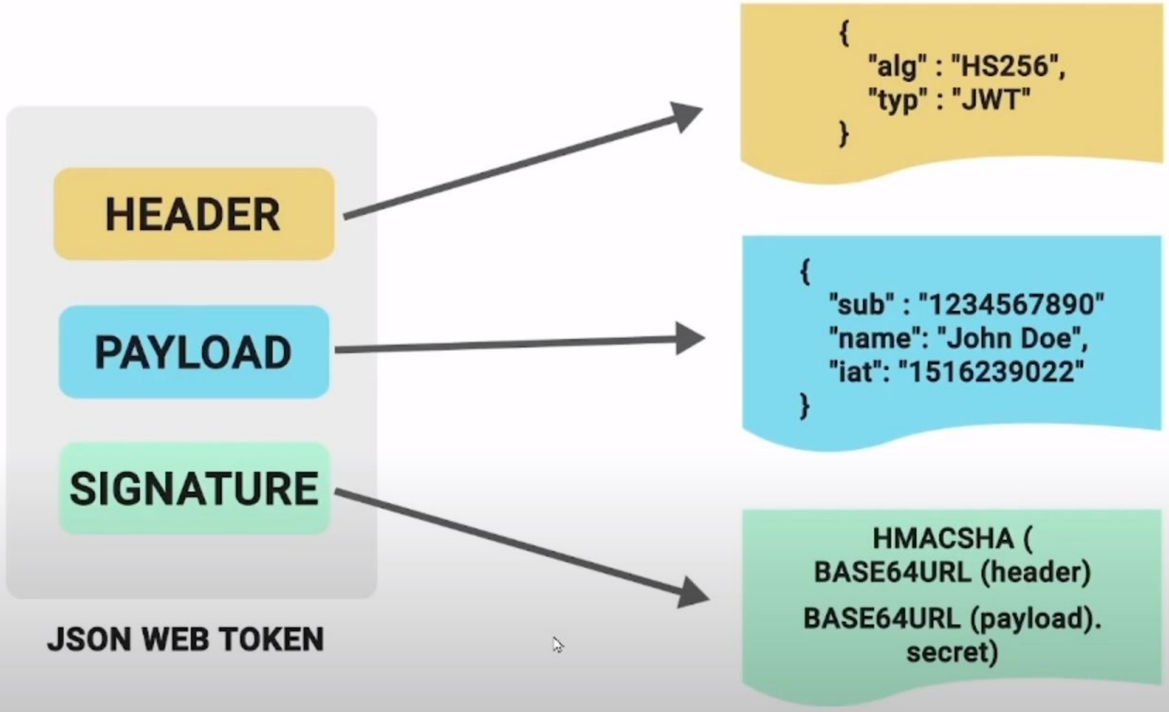
HEADER

PayLoad

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.
SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Signature

Structure of JSON Web Token (JWT)



HEADER

PAYLOAD

SIGNATURE

JSON WEB TOKEN

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

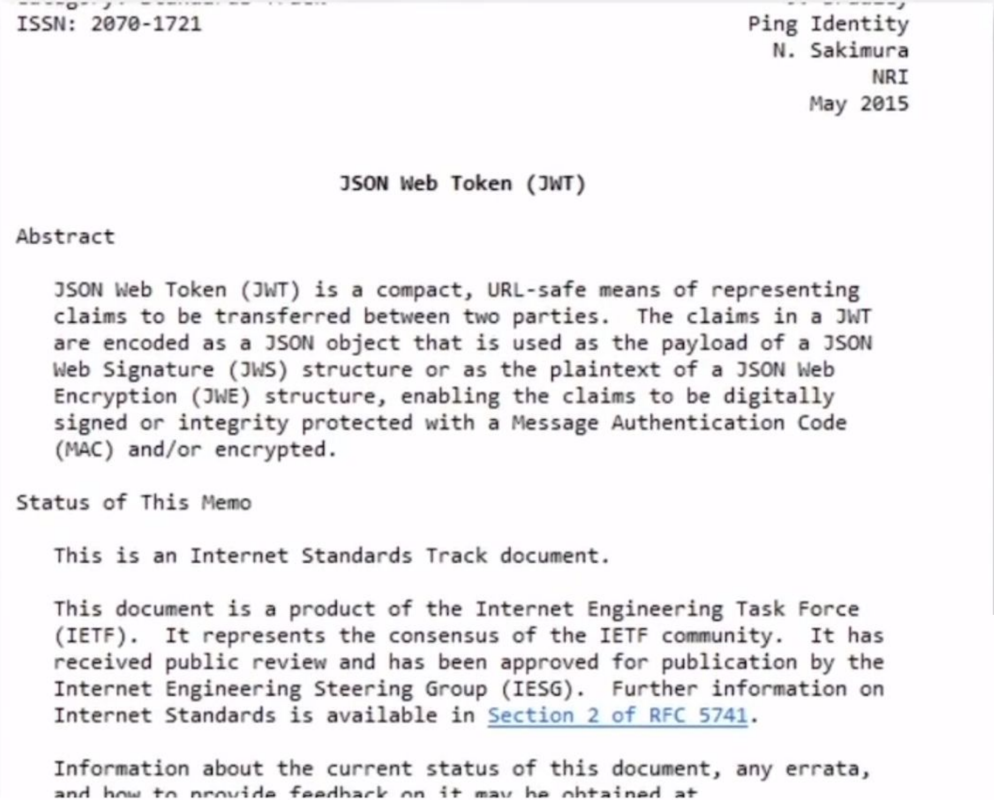
```
{
   "sub" : "1234567890"
   "name": "John Doe",
   "iat": "1516239022"
}
```

```
HMACSHA (
BASE64URL (header)
BASE64URL (payload).
secret)
```

SUMMARY

JSON Web Token

1. INDUSTRY STANDARD RFC 7519



Category: Standards Track
ISSN: 2070-1721

J. Bradley
Ping Identity
N. Sakimura
NRI

May 2015

JSON Web Token (JWT)

Abstract

JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

Status of This Memo

This is an Internet Standards Track document.

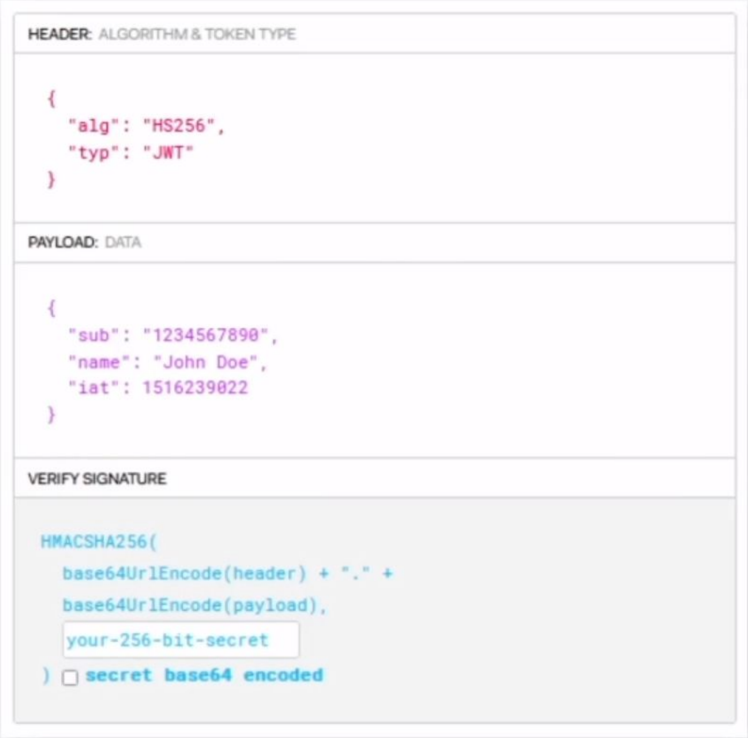
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at

SUMMARY

JSON Web Token

2. Securely transmits information between parties as a JSON object.



HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

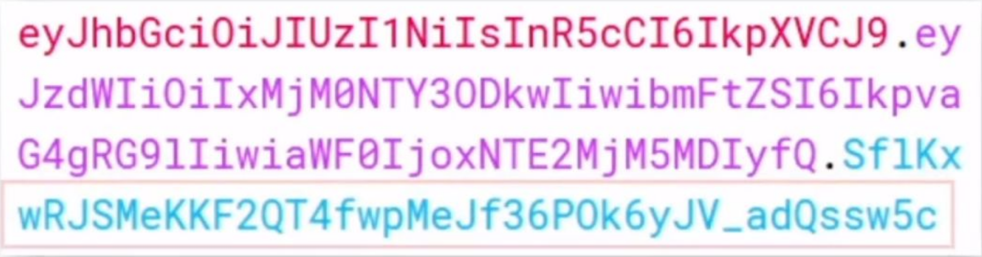
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

SUMMARY

JSON Web Token

3. Digitally Signed.



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```