Introduction to JWT (JSON Web Token), JWS (JSON Web Signature) and JWE(JSON Web Encryption)

Krishank Dwivedi Follow

Aug 10, 2018 · 2 min read

"JSON Web Token (JWT) or JOT is a Standard way (RFC 7919)of passing the information between different parties in the form of JSON we can Sign or Encrypt it if we sign the JWT it called JSON Web Signature (JWS) and If we Encrypt it become JSON Web Encryption (JWE) we can also Sign and Encrypt the JWT and then we call it JSON Object Signing and Encryption (JSOE)"

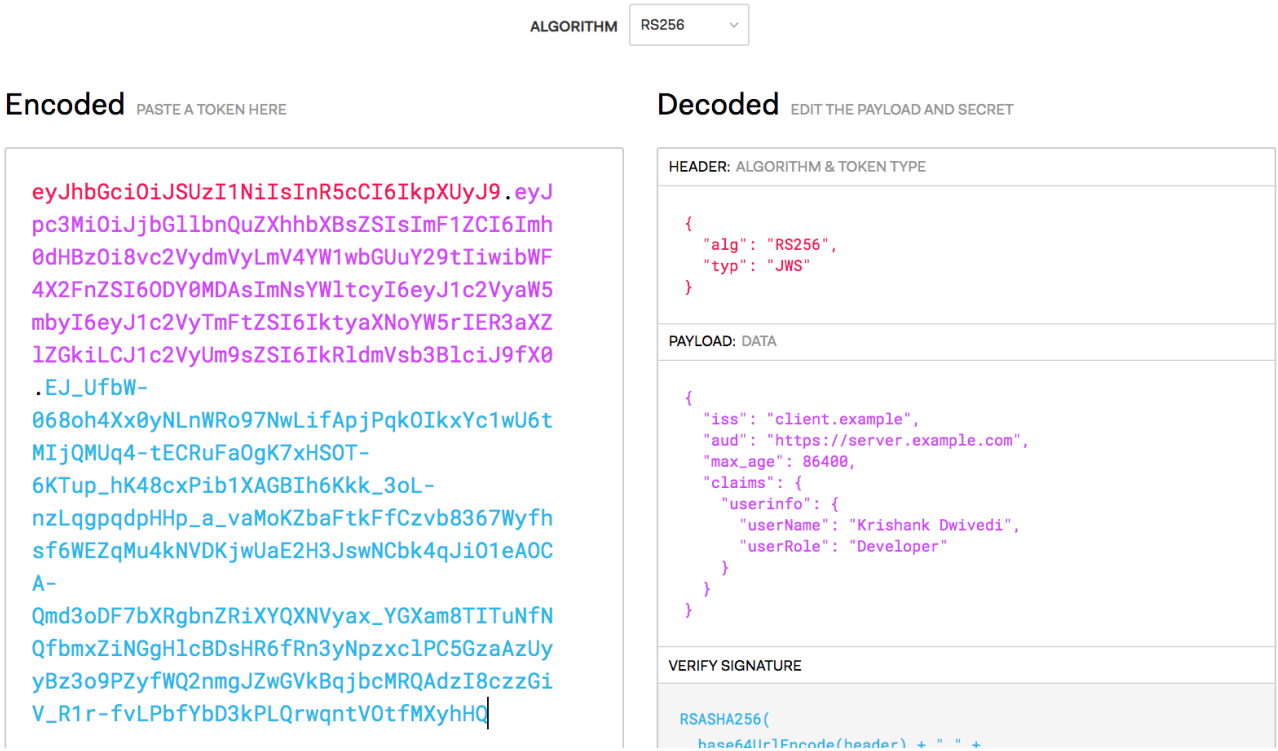
Use of JSON Web Token (JWT):

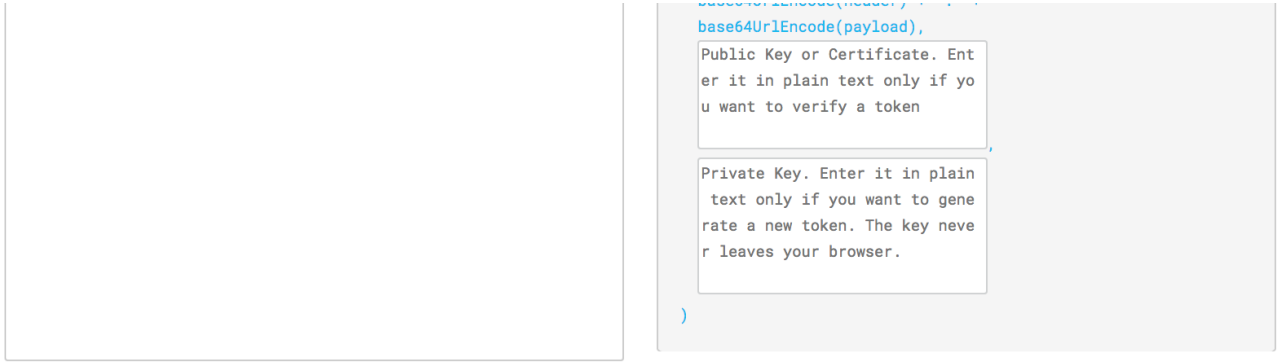
1. JWT is good for a Stateless implementation and the functionality like Single Sign On where we don't need a web server to create a sticky

session instead you can pass token in all subsequent request to access the resources permit for that token.

2. JWT is widely used to transfer the Secure Payload by Signing or Encrypting them this can be perform by using different Symmetric and Asymmetric Algorithms.

Structure of JSON Web Token (JWT): JWT is a combination of 3 parts which holds different informations **HEADER.BODY.FOOTER**.





Structure of JWT (JSON web token)

HEADER: Usually JWT header Contains the Information about the Type of JWT (JWT, JWS or JWE) and the hashing algorithm and then it is base64encoded.

PAYLOAD: Payload has the actual claims there are few claim which are mandatory and some are optional you can find more details here JWT Claims. On high level we can divide the Payload claims in 3 categories.

Registered claims: These Claims are not Mandatory or Optional the Applications using JWT have to define which of the Registered claims are Mandatory or Optional.

- `iss` : Who issues the Token

- `sub` : The subject of the token
- `aud` : Token is Issued For
- `exp` : When the Token will be Expire and the time is in NumericDate value you can convert it in readable format from here.
- `nbf` : The token Should not Use before this time.
- `iat` : JWT Creation Time.
- `jti(JWT Id)` : Unique identifier for the JWT. Can be used to prevent the JWT from being replayed. This is helpful for a one time use token.

Public Claims: These are the claims we define like user name, information, and other important information for more information click here.

Private Claims: A producer and consumer may agree to use claim names that are private like user IDs, user roles, or any other information. These are subject to collision, so use them with caution, for more information click here.

SIGNATURE:

This is the final and last part of a JWT which is actually a Hash of header, payload and secret.

JSON Object Signing and Encryption: There is an another type of token called JSON Object Signed and Encrypted (JOSE) this has many flavours which includes multiple combination of JWS, JWE, JWK (JSON Web Key), JWA (JSON Web Algorithm) to secure the content read more about JOSE specification here.

JavaScript Jwt Json Web Token