**JSON Web Token (JWT) is quite popular and used for Authentication -** Kevin Comba Jun 6, 2022

✍🏻 It’s a token-based standard that allows us to securely transfer information between two parties without storing anything in a database.

JWT token consists of three parts:  
✔️ Header  
✔️ Payload  
✔️ Signature  
Each one being BaseURL64 encoded to form the token.

𝐉𝐖𝐓 𝐚𝐮𝐭𝐡𝐞𝐧𝐭𝐢𝐜𝐚𝐭𝐢𝐨𝐧 𝐟𝐨𝐥𝐥𝐨𝐰𝐬 𝐚 𝐬𝐢𝐦𝐩𝐥𝐞 4 𝐬𝐭𝐞𝐩 𝐩𝐫𝐨𝐜𝐞𝐬𝐬

1) Client (Browser) sends post request with credentials to auth server to authenticate themselves

2) Auth Server authenticates user credential and generates a JWT. Server does not store anything and sends the token to the browser to save. It allows users to authenticate without their credentials in the future. It’s best advised to store the token in an http only cookie.

3) Thereafter for every request the client sends the JWT in the authorization header. Validation happens using token introspection with the auth server.

4) Once validated, resource server sends the necessary data to the client.

This covers a basic understanding of how JWT works. There’s much more to it.

Graphical user interface

Description automatically generated