JWT

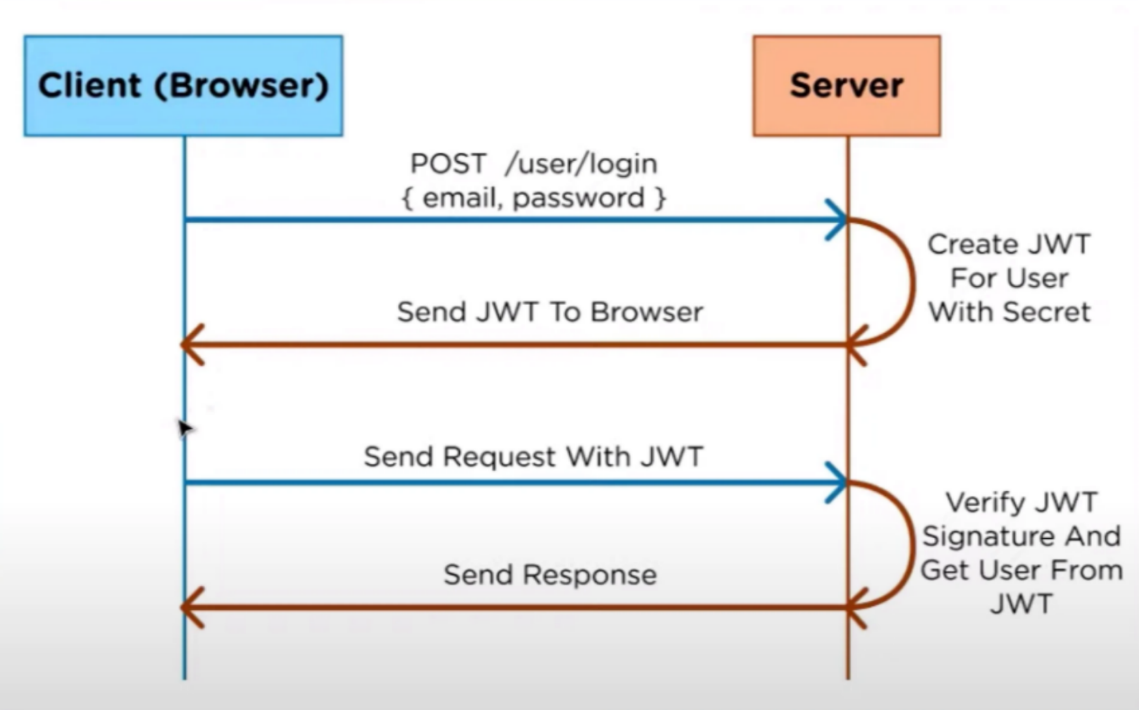
1. What is JWT?

According to Internet Engineering Task Force (IETF)

“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 JS 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”

1. When should I use JWT?

* Authorization

Common way of using JWT is authorization. After the user logs in to the application that user’s requests will have JWT, so the user is only available to access the things that are accessible with that token.

* Information Exchange

JWTs are a secure way to transfer information. With public/private keys users can make sure the receivers are correct and receivers can make sure that the information isn’t altered with.

1. Structure of JWT

In its compact form, JSON Web Tokens consist of three parts separated by dots (.), which are:

* Header

Headers has two parts one is the type of the token (JWT) and the algorithm that is used HMAC, RSA…

* Payload

Payloads include claims (issuer, expiration time, subject, audience). There can be some extra claims (defined as custom claims) like user role.

* Signature

Signatures are used the verify the issuer of JWT and check if the messages are altered with or not. Signatures are created when the encoded header/payload gets signed by the signature algorithm in the header.

Graphical user interface, text

Description automatically generated

Diagram

Description automatically generated

1. Why JWT?

JSON is neater than its competitors so in an encoded form its smaller in size and this also makes it good to pass in environments like HTML or HTTP. It has less chance of producing security holes. Because its easier to work with than SAML its more common. Also, it’s easier to process on user’s devices considering it is used at internet scale.

So JWT is

* More compact
* More secure
* More common
* More processable

DOT framework Chosen Research Methods:

* Available product analysis
* Community research
* Document analysis
* Ethical check
* Peer review

Resources:

* <https://datatracker.ietf.org/doc/html/rfc7519>
* <https://jwt.io/introduction>
* <https://auth0.com/docs/secure/tokens/json-web-tokens>
* <https://www.educative.io/edpresso/why-should-you-use-jwts>
* <https://www.ibm.com/docs/en/cics-ts/6.1_beta?topic=cics-json-web-token-jwt>
* <https://www.youtube.com/watch?v=DPrhem174Ws>