JWT

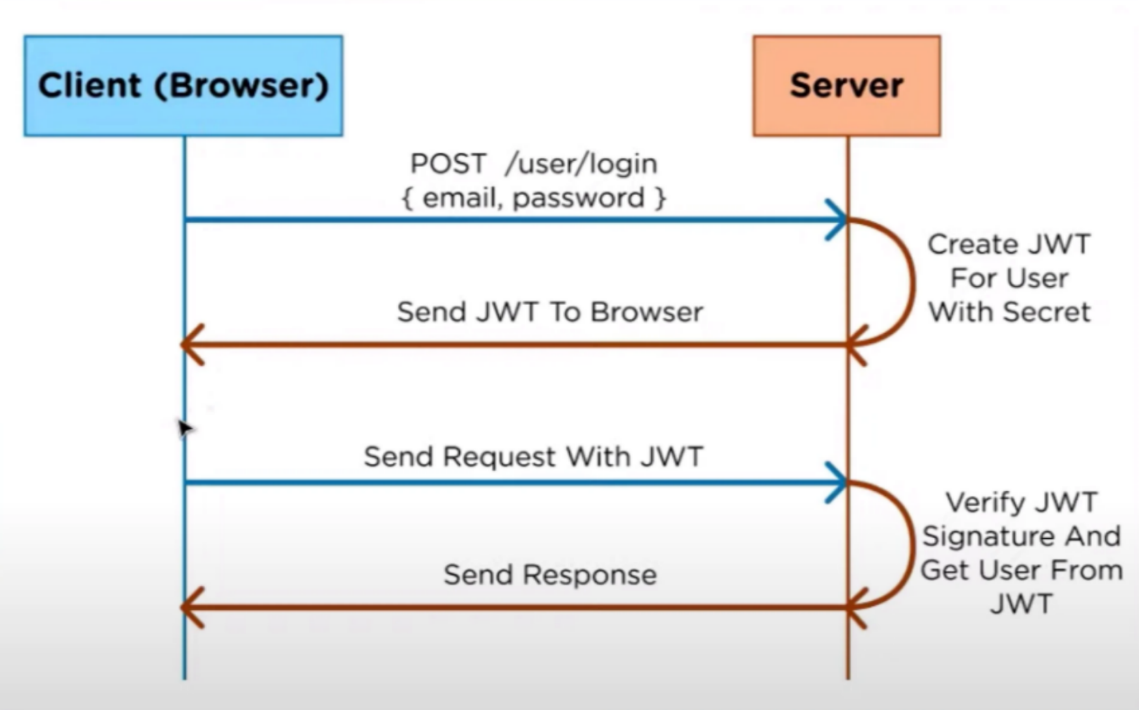
1. What is JWT?

According to the 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

A common way of using JWT is authorization. After the user logs into the application, that user’s requests will have a JWT, thus 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 data is not altered.

1. Structure of JWT

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

* Header

Headers have two parts: the type of the token (JWT) and the algorithm used (e.g., HMAC, RSA).

* Payload

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

* Signature

Signatures are used to verify the issuer of JWT and check if the messages are altered 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 should I use JWT?

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

So JWT is

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

Feedback:

I talked with Mr. Ligthart and Mr. Samuil, and they both provided me with the same feedback about confirming the truth of information by testing different technologies and writing my observation about those as proof. They also showed me APA Style Reference Citations.

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>
* <https://ictresearchmethods.nl/Methods>