**JSON Web Tokens (JWT)**

Is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as JSON object.

JWTs can be signed using a secret (with HMAC algorithm) or a public/private key pair using RSA.

Can be sent through an URL, POST parameter, or inside an HTTP header.

**When should you use JWTs?**

* Authentication
* Information Exchange

**Structure**

* **Header**: Has two parts, the type of the token and the hashing algorithm

Graphical user interface, text

Description automatically generated with medium confidence

* **Payload:** Contains the claims, these can be reserved, public and private claims.
  + **Reserved claims:** Some of them are **iss**(issuer)**, exp** (expiration time), **sub** (subject),  **aud** (audience).
  + **Public claims:** to avoid collisions they should be defined in the IANA JSON Web Token Registry or be defined as a URI that contains a collision resistant namespace.
  + **Private claims:** These are the custom claims created to share information between parties that agree on using them.

**Text

Description automatically generated**

* **Signature:** To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that.

Graphical user interface, text

Description automatically generated with medium confidence

Since tokens are credentials, great care must be taken to prevent security issues. In general, you should not keep tokens longer than required.