**Json Web Token**

Json Web Token (JWT) est un standard (RFC 7519) qui définit une solution **compacte** et **autonome** pour transmette de manière sécurisée des informations entre les applications en tant qu’objet structuré au format JSON (Java Script Object Notation)

Cette information peut etre **vérifiée** et **fiable** car elle est **signée** **numériquement**

**Compact :** en raison de leur petite taille, les JWT peuvent etre envoyés via une URL, un parametre POST ou dans un en tete HTTP. De plus , la plus petite taille signifie que la transmission est rapide.

**Autonome** : Le JWT contient toutes les informations requises sur l’utilisateur, ce qui évite d’avoir à interroger la base de données plus d’une fois pour connaitre le détail de l’identité d’un client authentifié.

DB

Serveur D’application

Client

HTTP

Socket

Socket

Connexion

GET/Login?

username=xpass=y

**Json Web Token**

JWT est composé de trois parties

{

"alg":"HS256",

"typ":"JWT"

}.

{

"sub": "1234567890",

"iss": "Backend",

"aud": "["Web Front End","Mobile App" ]",

"exp": 54789005,

"nbf": null,

"iat": 49865432,

"jti": "idr56sd66662121",

"name": "YZR",

"roles": ["admin","author"]

}.

{

C’est la signature = HMCHA256(base64UrlEncode(header)+"."+ base64UrlEncode(payload) , secret)

}

SQL

Header

**Géneration de Toker JWT en calculant Une signature Basée sur un secret**

200 Ok

Index.html

Jwt Header = H.P.S

Déconnexion

Payload

Socket

Socket

Nouvelle Connexion

**Verifier la signature du JWD en utilisant Le secret**

JWT Header:H.P.S

Réponse HTTP2

Requete HTTP2: POST/Save

Vue confirmation de l’enregistrement

Déconnexion

Signature