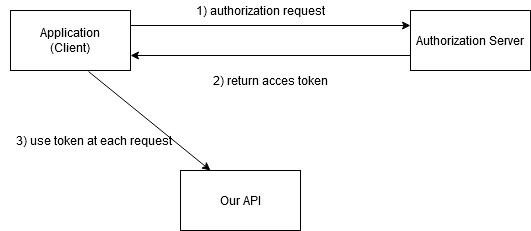
1. **Structure d’un jwt**

Un jwt est composé de trois parties séparées par des point :

* Header : composé de deux parties : le type de token (jwt), et l’algorithme utilisé (encodé en base 64)
* Payload : représente les données à transmettre (encodé en base 64). Parmi celle-ci il y a les registered claims qui permettent de déterminer le temps d’expiration du token, le créateur de celui-ci etc. Les private claims, qui sont les données d’information rajoutés.
* Signature : permet de vérifier l’intégrité des données

1. **Utilisation d’un JWT avec une API**

****

1. **Quel Algorithme choisir ?**

Il vaut mieux choisir un algorithme asymétrique qui utilisera (clé privé/public) en effet ces algorithmes permettent de limiter la connaissance de la clé privée uniquement au serveur d’authentification.

Par exemple RS256

1. **Précaution d’utilisation**

Il faut utiliser un protocole de communication sécurisé (HTTPS) car le jwt est uniquement encodé en base 64 et donc lisible par tout le monde.

La clé secrète qui permet de créer des tokens doit être conservée de façon extrêmement sécurisée. Sinon on pourrait créer des JWT reconnus et valide.

5)

pyjwt