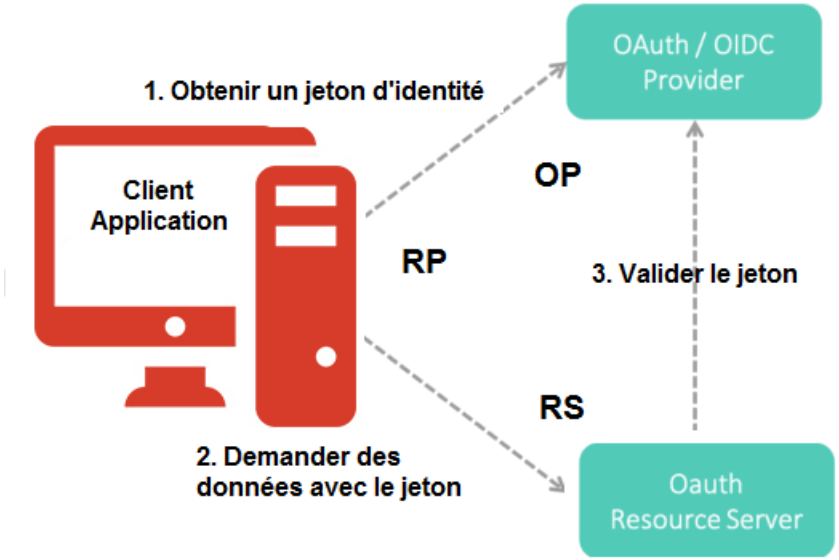
Politique d’entreprise :
l’authentification par jeton

Principes de base

Définition

L’authentification par jeton s’appuie sur un protocole qui permet à un utilisateur de **recevoir un jeton d’accès unique après avoir confirmé son identité**.

L’utilisateur bénéficie alors, pendant toute la durée de vie du jeton, d’un accès à l’application ou au site web pour lequel le jeton lui a été accordé et ce sans saisir ses identifiants à nouveau.



Concepts

Caractéristiques essentielles :

- Le jeton n'est valide que durant un **temps défini** et il s'invalide dès la sortie de l'application.
- L'authentification par jeton est appelé **authentification « forte »** et diffère du mécanisme traditionnel du mot de passe.
- Les jetons peuvent être **par connexion** (clés, cartes, etc.), **sans contact** (biométrie), **à distance** (via un autre appareil).

SecurID

Clé usb

Carte à puces

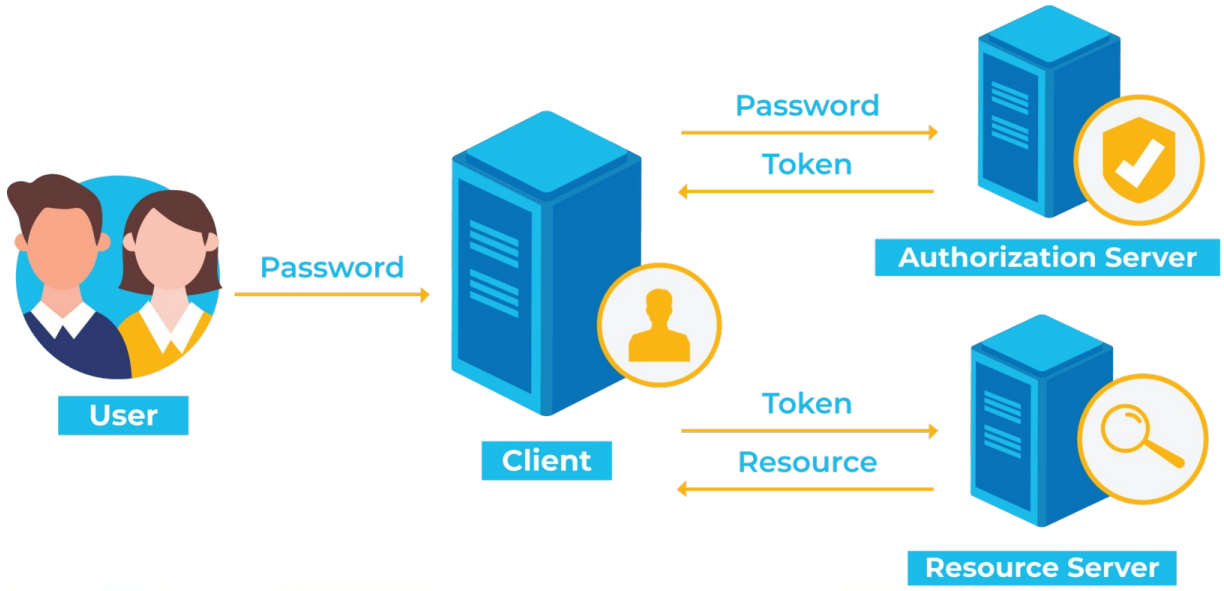
Serveur VPN

Les étapes

Rappel : les identifiants des utilisateurs ne sont vérifiés qu'une seule fois, avec attribution d'un jeton garantissant un accès continu pendant une période définie.

Déroulement de la procédure :

- **Requête** : demande d'accès à un serveur ou à une ressource protégée par l'utilisateur.
- **Vérification** : le serveur détermine si l'accès doit ou non être accordé à cette personne.
- **Génération du jeton** : le serveur émet un jeton et l'envoie à l'utilisateur.
- **Stockage** : le navigateur de l'utilisateur conserve le jeton pendant toute la durée nécessaire.



Pourquoi utiliser un jeton ?

Pour des accès temporaires : dans le cas par exemple d'une base utilisateurs liées à un horaire (bibliothèques , etc...).

Pour des accès spécifiques : en fonction par exemple d'un document au lieu d'un rôle utilisateur ; chose que les mots de passe ne permettent pas.

Pour une sécurité accrue : on choisira dans ce cas un équipement matériel comme une clé n supplémentaire.

L’authentification JWT

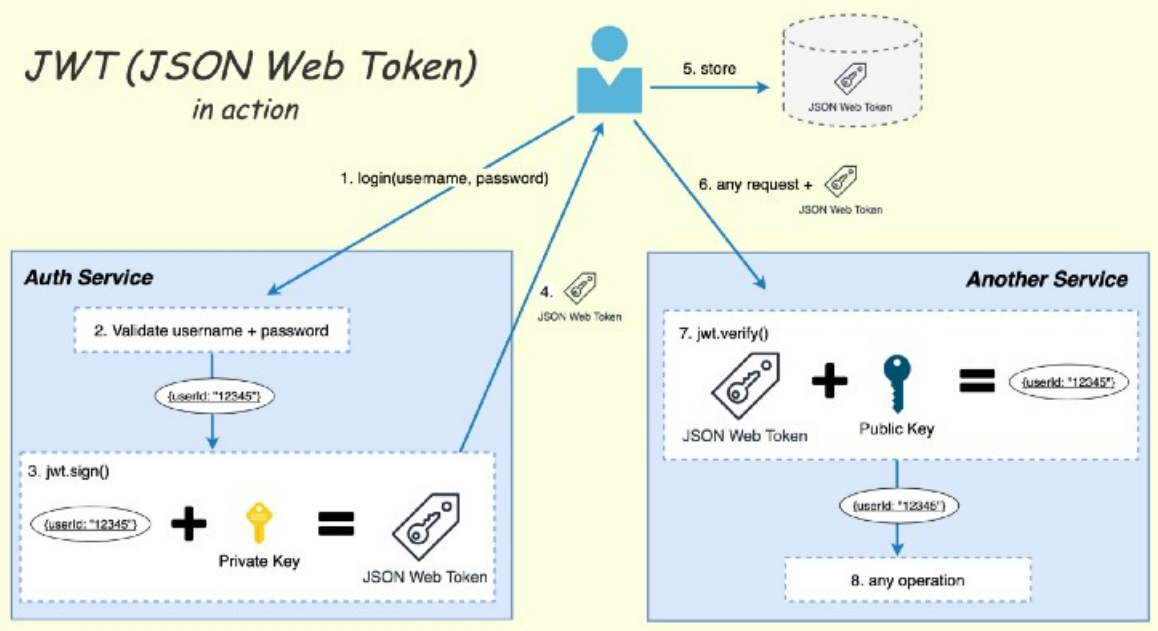
JSon Web Token est une norme ouverte plus spécifiquement adaptée aux applications Web et mobiles. Les données sont vérifiés à l’aide d’une signature numérique et transmise par HTTPS.

Trois composants importants :

- **En-tête** : donne le type de jeton et son algorithme de signature.
- **Données** : précisent l’émetteur du jeton, sa date d’expiration, etc...
- **Signature** : vérifie la non modification du message pendant l’échange.

Ressource :

https://jwt.io/introduction/



Avantages et inconvénients

Avantages :

- **Taille** : les jetons en JSon sont de très petites tailles, donc facilement transmissibles.
- **Simplicité** : les jetons se génèrent partout et sans vérification de votre serveur.
- **Contrôle** : les jetons contrôlent le droit d'accès, la période autorisée et les actions possibles.

Inconvénients :

- **Clé unique** : les jetons reposent sur une clé unique, donc tout le système devient vulnérable en cas de compromission.
- **Complexité** : les jetons nécessitent de bonnes connaissances du développeur (algorithmes de signature cryptographique).
- **Limites** : il n'est pas possible d'envoyer les messages automatiquement à tous les clients ni de gérer les clients côté serveur.