Convergence processus CFA/OPCO
Description technique de l'authentification

Mises à jour			
Version	**Date**	**Auteur**	**Motifs**
1.0	02/06/2021	TCO	Création
1.1	23/07/2021	TCO	Précisions sur l'API Key
1.2	16/01/2024	AAM	Mise à jour : durée de validité d'un Token

Objectif du document

L'objectif de ce document est de présenter dans les grandes lignes le fonctionnement de l'authentification et de proposer des pistes dans la mise en œuvre de celle-ci dans le cadre du projet de convergence des processus CFA/OPCO.

Authentification

L'authentification se découpe en deux éléments principaux : l'authentification du SI du CFA grâce à OAuth2.0 (via le *Client Credentials Flow*) et l'authentification du CFA via une *API Key*.

Trois étapes constituent la cinématique globale et seront décrites dans ce document :

- Obtention du *Client Id* et *Client Secret*
- Obtention de l'*API Key*
- Authentification des appels

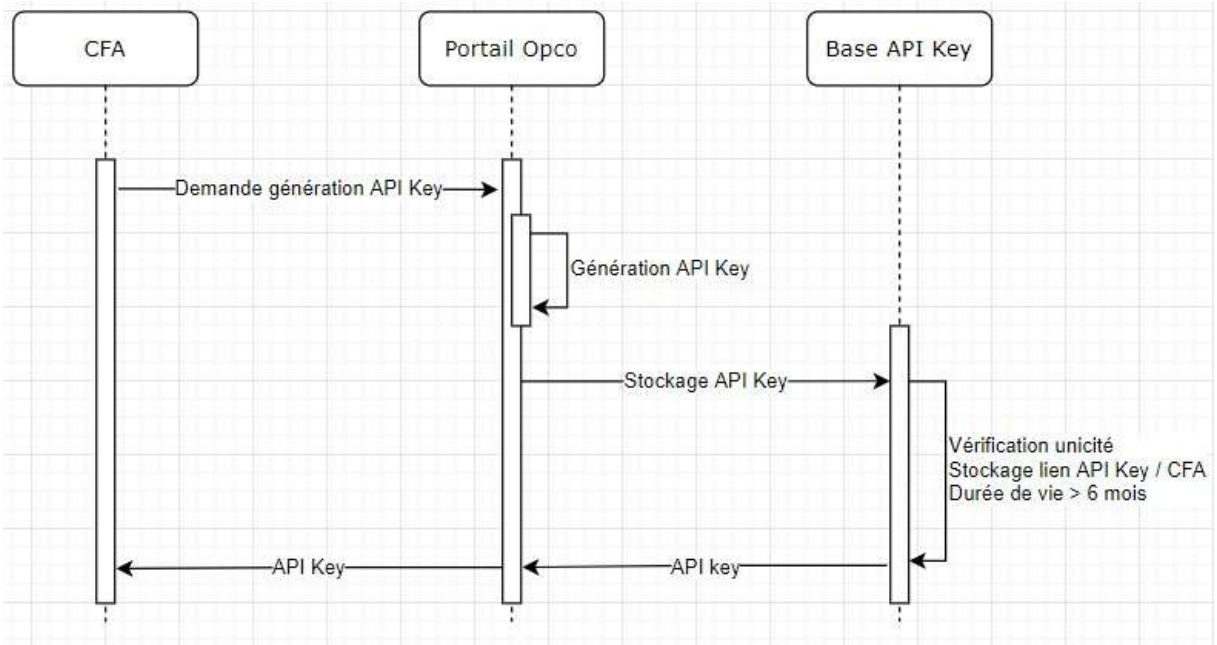
Obtention du Client Id et Client Secret

Les *Client Id* et *Client Secret* désignent des éléments du protocole OAuth2.0 et notamment du *Client Credentials Flow* utilisé par cette API.

Des couples *Client Id / Client Secret* sont attribués à chaque SI CFA et permettent à ceux-ci de s'authentifier auprès des SI des OPCO (authentification *system to system)*. Ces identifiants ne permettent pas d'authentifier le CFA en tant qu'utilisateur de l'API.

Les *Client Id* et *Client Secret* sont créés par les OPCO (via un *Authorization Server*) et mis à disposition des éditeurs de SI CFA. Ils sont utilisés par ces derniers pour obtenir un *Bearer Token* via un appel webservice. Ce *Bearer Token* sera à passer en paramètre de chaque requête dans l'entête **Authorization**.

Obtention de l'API Key



L'API Key est une clé unique à chaque CFA. Elle permet d'identifier le CFA et donc de vérifier ses habilitations. Cette clé est liée au SIREN du CFA et lui permet donc d'accéder aux informations de tous les établissements liés à ce SIREN.

L'obtention de l'API Key doit être fait à chaque fois que sa durée de vie est dépassée ; celle-ci a été fixée à 6 mois minimum.

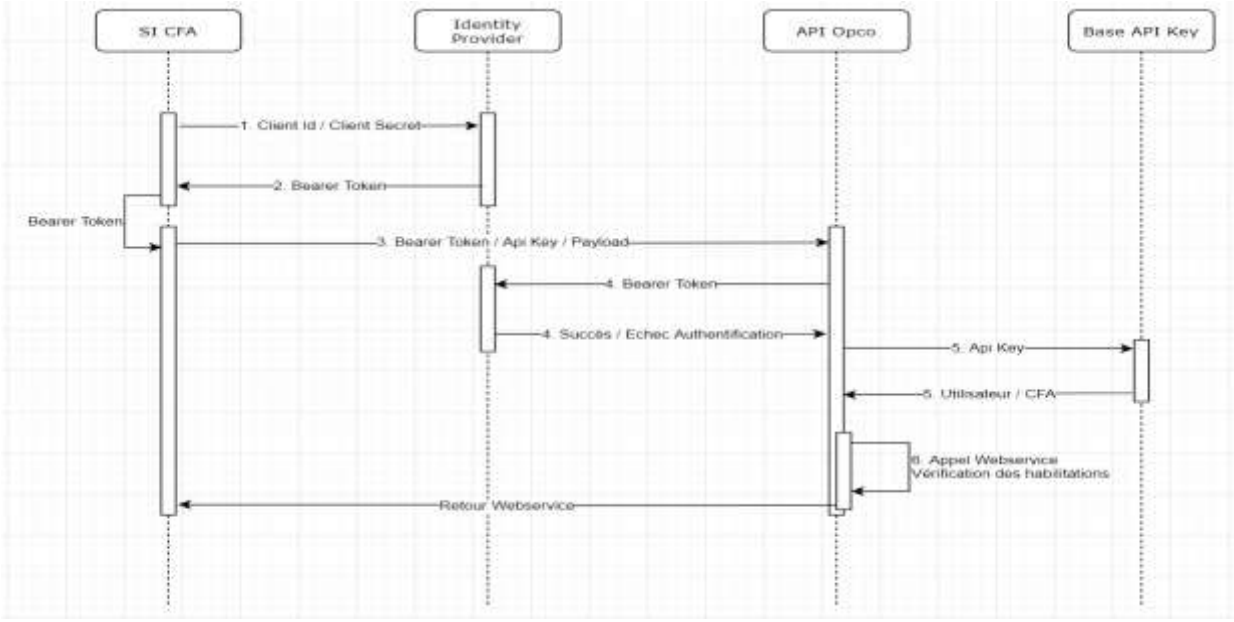
Via le portail mis à disposition par l'OPCO, le CFA fait une demande de génération d'API Key

- Le portail génère une API Key :
  - Unique par CFA
  - Aléatoire et/ou signée par une clé secrète (par exemple : un token JWT)
    - Il faut impérativement que cette API Key ne puisse pas être forgée par un tiers
  - Ayant une durée de vie supérieure à 6 mois
    - Cette durée de vie longue permet d'éviter au CFA d'avoir à mettre à jour trop régulièrement cette API Key
- L'API Key est stockée dans un lieu de stockage dédié (ici : Base API Key) avec les informations du CFA qui possède cette API Key et sa durée de vie
- L'API Key est renvoyée au CFA qui doit la paramétrer dans son SI

Remarque : Ce schéma présente le cas d'une clé unique générée aléatoirement et stockée par l'OPCO. Si l'OPCO choisissait de générer un token JWT, il pourrait s'affranchir du stockage de la clé en vérifiant que le token transmis par le CFA a bien été signé par sa propre clé secrète.

Les schémas suivants partent du principe que l'API Key est une clé aléatoire stockée par l'OPCO.

Authentification des appels WS



Prérequis 1 : Obtention du *Client Id* et du *Client Secret*

Prérequis 2 : Obtention de l'*API Key*

- L'*API Key* obtenue précédemment devra être renseignée dans une entête personnalisée **X-ApiKey** à chaque appel

À chaque appel d'API

1. Le SI CFA fait un premier appel à l'*Authorization Server* avec son *Client Id* et son *Client Secret* en paramètre
2. Si le *Client Secret* est connu de l'*Authorization Server*, celui-ci renvoie un *Bearer Token* qui devra être passé dans l'entête **Authorization** de chaque appel API (**60 minutes de validité pour chaque Token**)
   Chaque appel devra contenir :
   - Une entête **X-Api-Key** contenant l'*API Key* du CFA
   - Une entête **Authorization** contenant le *Bearer Token* du SI du CFA
   - Eventuellement un *Payload*
3. Le SI CFA appelle l'API mise à disposition par l'OPCO avec les informations précédentes
4. Le SI OPCO vérifie la validité du *Bearer Token* en faisant appel à l'*Authorization Server*
   - Si le *Bearer Token* est invalide, l'API renvoie une erreur 401 Unauthorized (non schématisé)
5. Le SI OPCO vérifie la validité de l'*API Key* en vérifiant l'existence de celle-ci dans la base *API Key* et sa durée de vie ○ Si l'*API Key* est inconnue ou qu'elle a expiré, l'API renvoie une erreur 403 Forbidden
   (non schématisé) ○ Si l'*API Key* est valide, les informations du CFA associé à cette *API Key* sont renvoyées au SI de l'OPCO
6. Grâce aux informations du CFA et au payload de la requête, l'OPCO peut vérifier que les opérations effectuées par un CFA sont permises (dépôt d'un contrat d'apprentissage, dépôt de facture, …)