



Je sais gérer des clefs API

☰ Flux	
# Durée [h]	
☰ Role	OpsBuild OpsRun
🕒 Last edit	@April 26, 2022 12:04 PM
☰ Property	

Le why

- On veut minimiser la transmission des clefs API pour réduire le risque de fuite
- En cas de fuite, on veut pouvoir identifier sans ambiguïté d'où la fuite provient
- En cas de fuite, on veut ne pouvoir révoquer qu'une seule clef afin de retrouver le fonctionnement nominal le plus rapidement possible

Livrables

- J'ai une clef API pour chaque usage
 - Une clef par application par environnement (une clef pour l'application en prod, une différente pour la preprod, une différente pour la dev et cela pour chaque application)
- Une clef par personne qui a besoin de s'en servir en local

Erreurs à éviter

- Utiliser la clef d'une application pour tester depuis mon ordinateur local

- Utiliser la même clef pour 2 applications
- Utiliser la même clef sur deux environnements
- Donner sa clef à quelqu'un "juste pour tester"
- Envoyer une clef en clair dans un mail/message Slack/autres...
- Commiter la clef dans un repository (privé ou public)
- Transmettre dans le même message les clefs pour chaque environnement d'une application
- Envoyer la clef qui doit être déployée dans un environnement à un développeur
- Ne pas révoquer une clef lorsqu'un tech ne fait plus partie du projet
- Ne pas renouveler les clefs lorsqu'un tech qui y a eu accès quitte le projet

Prérequis

- J'utilise un service qui nécessite une clef API

Étapes clefs

Transférer la clef de manière sécuriser

- Je vais sur [Yopass](#)
- Je copie la clef dans le champ texte
- Je coche la case **One-time download**
- Je coche la case **Generate decryption key**
- Je génère un lien valide **1h**
- J'envoie le lien par mail
- J'envoie la **clef de décryptage par SMS**

Je dois générer une clef pour un développeur afin qu'il puisse tester en local

- Je génère la clef API
- Je suis la procédure d'envoi et ne transmet les infos qu'à la personne qui en a besoin

Je dois générer la clef pour une application

- Je génère une clef par environnement
- J'envoie la clef à un Ops qui doit se synchroniser avec le développeur pour savoir comment la déployer
- Je suis la procédure d'envoi une fois pour chaque environnement en précisant quelle clef doit être utilisée sur quel environnement
- L'Ops intègre les clefs dans les différents environnements

Un tech quitte le projet

- S'il a une clef personnelle, il faut la révoquer
- S'il s'agit d'un Ops qui a eu accès aux clefs d'un cluster, il faut **toutes** les renouveler