Certificat

**Pour sécuriser on a besoin d’utiliser un certificat, ce qui demande plusieurs étapes que je vais décrire ici :**

## Créer une demande de signature de certificat

Je génère une clé privée et une demande de signature de certificat (ou CSR) en exécutant la commande suivante :

Une image contenant texte

Description générée automatiquement

Cette commande génère deux fichiers ; il génère server.csr contenant la demande de certification server-key.pem encodée PEM et contenant la clé encodée PEM du certificat qui reste à créer.

## Créer un objet CertificateSigningRequest à envoyer à l'API Kubernetes

Je génère un manifeste CSR (en YAML) et je l’envoie au serveur d'API :

Une image contenant texte

Description générée automatiquement

Le CSR devrait maintenant être visible depuis l'API dans un état En attente. Avec la commande :

kubectl describe csr my-svc.my-namespace

## Faire approuver la CertificateSigningRequest

L'approbation de la demande de signature de certificat est effectuée un administrateur de cluster. Je le fais manuellement :

kubectl certificate approve my-svc.my-namespace



Cela signifie que la demande de certificat a été approuvée et attend que le signataire demandé la signe.

## Signer le CertificateSigningRequest

Ensuite, je joue le rôle d'un signataire de certificat, j’émets le certificat et je le télécharge sur l'API.

## Créer une autorité de certification

J’ai besoin d'une autorité pour fournir la signature numérique sur le nouveau certificat :

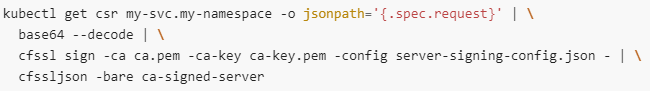
Une image contenant texte

Description générée automatiquement

Cela produit un fichier de clé d'autorité de certification ( ca-key.pem) et un certificat ( ca.pem).

## Délivrer un certificat

J’utilise un server-signing-config.jsonconfiguration de signature et le fichier de clé et le certificat de l'autorité de certification pour signer la demande de certificat :



Cela produit un fichier de certificat de service signé, ca-signed-server.pem

## Télécharger le certificat signé

Enfin, je remplis le certificat signé dans le statut de l'objet API :



Avec la commande kubectl get csr



## Téléchargement du certificat et utilisation

je télécharge le certificat émis et l'enregistre dans un server.crt en exécutant ce qui suit :



Maintenant, je peux remplir server.crt et server-key.pem dans un Secret que mets ensuite dans un pod pour https.



Au final je rajoute quelques lignes dans l’ingress pour la cohérence des clés, et surtout je change les ports, de 80 (http) vers 443 (https).