

Let's Encrypt

Introduction

L'objectif de cette page est de générer et faire signer des certificats avec Let's Encrypt. Cette méthode n'est pas la plus simple, mais elle permet de mettre en place [DANE/TLSA](#) et [HPKP](#) ainsi que d'avoir des certificats en [ECC](#).

Pour cela, il faut juste le paquet certbot/letsencrypt.

Cette méthode n'est pas éligible au renouvellement automatique de certbot, donc il faudra ajouter manuellement l'entrée en tâche cron. La méthodologie, si suivie à la lettre, permet une gestion simple de ces certificats.

Génération du certificat

Pour chaque domaine, nous allons créer les dossiers où seront stockés les certificats et les clés:

```
# mkdir -p /etc/letsencrypt/wiki.virtit.fr/live
# mkdir -p /etc/letsencrypt/wiki.virtit.fr/archive
```

puis on génère le certificat :

```
# openssl ecparam -name prime256v1 -genkey -out
/etc/letsencrypt/wiki.virtit.fr/live/private.key
# openssl req -new -key virtit.pem -nodes -days 3650 -out
/etc/letsencrypt/wiki.virtit.fr/live/cert.csr
```

Ces certificats seront uniques mais pensez à les renouveler régulièrement 😊.

Signature du certificat

Pour signer votre certificat, il faut lancer la commande suivante :

```
# certbot certonly --webroot -w /var/www/letsencrypt/ -d wiki.virtit.fr --
csr /etc/letsencrypt/wiki.virtit.fr/live/cert.csr --cert-path
/etc/letsencrypt/wiki.virtit.fr/live/cert.pem --chain-path
/etc/letsencrypt/wiki.virtit.fr/live/chain.pem --fullchain-path
/etc/letsencrypt/wiki.virtit.fr/live/fullchain.pem
```

Renouvellement du certificat

Pour renouveler le certificat, il faut déplacer le certificat, et les chaînes de certificats.

Je vous conseil d'ajouter la tâche **cron** suivante :

```
0 2 1 * * /bin/rm /etc/letsencrypt/wiki.virtit.fr/archive/* || true &&
/bin/mv /etc/letsencrypt/wiki.virtit.fr/live/*.pem
/etc/letsencrypt/wiki.virtit.fr/archive/ && /usr/bin/certbot certonly --
webroot -w /var/www/letsencrypt/ -d wiki.virtit.fr --csr
/etc/letsencrypt/wiki.virtit.fr/live/cert.csr --cert-path
/etc/letsencrypt/wiki.virtit.fr/live/cert.pem --chain-path
/etc/letsencrypt/wiki.virtit.fr/live/chain.pem --fullchain-path
/etc/letsencrypt/wiki.virtit.fr/live/fullchain.pem --post-hook
'/bin/systemctl reload apache2'
```

Il faudra adapter la dite commande avec le bon domaine et les bons post-hook.

From:

<https://wiki.virtit.fr/> - **VirtIT**

Permanent link:

<https://wiki.virtit.fr/doku.php/kb:crypto:letsencrypt?rev=1520691674>

Last update: **2018/03/10 14:21**

