HPKP

Comprendre HPKP

Compatibilité avec Let's Encrypt

HPKP est tout comme DANE_TLSA, nativement pas compatible avec **certbot**. Mais avec un peu de rigueur, et les bons arguments, on peut faire en sorte de garder ses clés publiques et donc permettre de garder ses empreintes **HPKP**. N'oubliez pas de faire un deuxième certificat non signé pour la backup.

Générer une entrée HPKP

Pour obtenir le **HASH** du certificat, il faut taper la commande :

```
# openssl req -pubkey < /etc/letsencrypt/wiki.virtit.fr/live/cert.csr |
openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | base64
```

et il suffira d'ajouter une entêtes suivante dans votre serveur WEB, par exemple pour apache :

```
Header always set Public-Key-Pins "max-age=5184000; pin-
sha256=\"JOLIE_PETIT_HASH_ACTIF\"; pin-sha256=\"JOLIE_PETIT_HASH_BACKUP\"; "
```