DANE/TLSA

Comprendre DANE/TLSA

🔧Fix Me!

Compatibilité avec Let's Encrypt

Une des spécificité de **certbot** est que à chaque renouvellement, le **CSR** est recréé et donc l'empreinte du certificat aussi. Ce qui voudrait dire qu'il faudrait donc changer l'entrée **DNS** tous les trois mois. 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 enregistrement **TLSA** à chaque renouvellement. Certe un oubli n'est pas critique à l'heure d'aujourd'hui car non supporté par les navigateurs.
Je vous renvoi vers Let's Encrypt

Génération une entrée

J'utilise l'outil **hash-slinger** qui permet de générer simplement ces enregistrements avec la commande suivante :

```
# tlsa --create --usage 1 --selector 1 --mtype 2 --certificate
/etc/letsencrypt/wiki.virtit.fr/live/cert.pem wiki.virtit.fr
```

Vérifier une entrée

Pour vérifier une entrée, il taper :

```
# tlsa --verify --port 443 wiki.virtit.fr
```

From:
https://wiki.virtit.fr/ - **VirtIT**

Permanent link:
https://wiki.virtit.fr/doku.php/kb:crypto:dane_tlsa

Last update: **2018/07/03 07:45**