DNSSEC

Générer des clés sécurisé

Pour générer une clé KSK avec l'algorithme 14 :

```
# dnssec-keygen -a ECDSAP384SHA384 -3 -n ZONE -f KSK -r /dev/urandom exemple.net
```

Pour générer une clé ZSK avec l'algorithme 14 :

```
# dnssec-keygen -a ECDSAP384SHA384 -3 -n ZONE -r /dev/urandom exemple.net
```

Signer une zone

```
# dnssec-signzone -3 1EA78EAF -e 20180806050000 -k
/etc/bind/keys/Kexemple.com.ksk.key -o exemple.com
/etc/bind/local/exemple.com /etc/bind/keys/Kexemple.com.zsk.key
```

Roll-Over des clés

- 1. Générer une nouvelle clé
- 2. Ajouter la clé dans la zone
- 3. Fournir l'entrée DS au registrar
- 4. Attendre le temps de déploiement et de fin de cache
- 5. Signer la zone avec la nouvelle clé et supprimer l'ancienne clé du registrar

Vérifier ses signatures

Afin de vérifier de manière graphique, voici un site fait pour cela :

http://dnsviz.net/

From:

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

Permanent link:

https://wiki.virtit.fr/doku.php/kb:crypto:dnssec?rev=1598781928

Last update: 2020/08/30 10:05

