# Signer ses entrées DNS avec DNSSEC sous Bind9


Gérer son DNSSEC est plutôt simple, mais demande de la précaution, car si vous faites une erreur, les résolutions DNS de votre domaine seront rejetées par les résolveurs.

## Signer un domaine

### Configuration de votre Bind9

Avant de commencer, il faut s'assurer de plusieurs choses. La première est qu'il faut impérativement que l'utilisateur de votre service **bind9** puisse écrire dans le dossier contenant les zones. Personnellement, je crée un dossier **/var/lib/bind9/zones** appartenant à l'utilisateur **bind**, et je fais un lien symbolique pour qu'il apparaisse aussi dans le dossier **/etc/bind/**.

Il faudra ensuite définir un dossier pour contenir les clés. Ce dossier devra est lisible par l'utilisateur de votre service **bind9**. Dans la configuration, dans la catégorie options, vous devrez donc définir :

```
key-directory "/etc/bind/keys";
```

Ensuite, je vous conseille de définir la méthode de mise à jour des zones en mode date, ce n'est pas obligatoire, mais je préfère comme ça. Dans votre configuration, toujours dans la catégorie **options**, il vous faut simplement définir :

```
serial-update-method date;
```

### Configuration de votre domaine

Pour commencer, il faut générer les clés pour ce domaine. Avant cela, il faut il faut générer.

Pour générer une clé KSK avec l'algorithme 16 :

```
# dnssec-keygen -a ED448 -3 -n ZONE -f KSK exemple.net
```

Pour générer une clé ZSK avec l'algorithme 16 :

```
# dnssec-keygen -a ED448 -3 -n ZONE exemple.net
```

Ensuite, dans la déclaration de votre zone dans la configuration de **bind9**, il faudra inclure ces deux lignes :

```
auto-dnssec maintain;
```

```
inline-signing true;
```

Et recharger **bind9** avec :

```
# rndc reload
```

Une fois fait, vérifiez que votre domaine est bien signé en faisant une requête DNS simple :

```
# dig +short @ns01.virtit.fr virtit.fr DNSKEY
```

Vous devriez voir vos 2 clés:

```
257 3 14 8EFFgoNyjBNEVEJv2bcWEuJNVce/UAEFLUmImpSbXoheyMxPZie7XGLW
lr7JK0kxt/LqHz5vIqNq5dmjLMOKLo+sziw8/Xn03aM+RdAOOPO9YYQk zMMf5x49kbGRE0UQ
256 3 14 hnBDXcku9GgDVcs+UjwE837AXqkg22dzNDRy9ovb+JgOPUSJxggyTpos
DorqO+C5zklhUQQGdS59fNiL+9w/jcGNAEj6d/vkO941KuH0M1WxkP1u WkDidQEnvXKYMu3d
```

Ensuite, comme quand vous avez créé vos clés, il va falloir aller définir les entrées DS dans votre registrar. Il est obligatoire de déclarer les entrées DS de ses clés KSK, et facultatif de le faire pour les clés ZSK. La norme étant même de ne pas le faire.

Pour récupérer l'entrée DS, faites la commande :

```
dnssec-dsfromkey -a SHA-384 Kvirtit.fr.+016+17928.key
```

et ensuite, on va l'ajouter dans votre registrar. Il m'est impossible de couvrir tout les registrar, donc a vous de trouver comment faire.

Une fois fait, vous pouvez vérifier que les signatures sont valides via le site https://dnsviz.net/

## Roll-Over des clés

La pratique recommandée est de renouveler ses clés ZSK tout les 3 mois, et les KSK tous les ans.

Personnellement, je ne prends pas le temps de le faire, je fais le renouvellement des 2 clés tous les ans environ.

Rendez-vous dans votre dossier de clé, et générez les clés que vous souhaitez renouveler. Comme ceci pour la KSK :

```
# dnssec-keygen -a ED448 -3 -n ZONE -f KSK -r /dev/urandom exemple.net
```

et comme cela pour la ZSK:

```
# dnssec-keygen -a ED448 -3 -n ZONE -r /dev/urandom exemple.net
```

Assurez vous que les clés sont lisibles par l'utilisateur de **bind**, dans mon cas, il suffit d'autoriser la lecture au groupe, via :

```
# chmod g+r /etc/bind/keys/*
```

Ensuite, rechargez la configuration de bind :

```
# rndc reload
```

Ensuite, vous pouvez vérifier que les clés ont été chargées via :

```
# dig +short @ns01.virtit.fr virtit.fr DNSKEY
```

Vous devriez voir 4 clés, les anciennes et les nouvelles, par exemple :

```
257 3 14 8EFFgoNyjBNEVEJv2bcWEuJNVce/UAEFLUmImpSbXoheyMxPZie7XGLW
lr7JK0kxt/LqHz5vIqNq5dmjLMOKLo+sziw8/Xn03aM+RdAOOPO9YYQk zMMf5x49kbGRE0UQ
256 3 14 hnBDXcku9GgDVcs+UjwE837AXqkg22dzNDRy9ovb+JgOPUSJxggyTpos
DorqO+C5zklhUQQGdS59fNiL+9w/jcGNAEj6d/vkO941KuH0M1WxkP1u WkDidQEnvXKYMu3d
256 3 16 qI8l3+HET31u9qSw3l8mjKVoM0QI6dRlHAH2j/VySfM7cc4FakesgoT7
4Kj8tIDWShTIAbQ8gh2A
257 3 16 XKBH2mz7VoHzOPxcYPAqfjxr9yAu3Xweu7pGSGhxxQx7TJilIYj0f1zV
uqFh7TQ6cmdna3HPrbaA
```

Ensuite, comme quand vous avez créé vos clés, il va falloir aller définir les entrées DS dans votre registrar. Pour rappel, il est obligatoire de déclarer les entrées DS de ses clés KSK.

Pour récupérer l'entrée, faites la commande :

```
dnssec-dsfromkey -a SHA-384 Kvirtit.fr.+016+17928.key
```

et ensuite, on va l'ajouter dans votre registrar. Il m'est impossible de couvrir tout les registrar, donc a vous de trouver comment faire.

 Ne supprimez pas les anciennes entrées DS pour le moment

Il faudra attendre l'expiration du TTL de vos entrées DS, ce qui dépend de votre registrar. Vous pouvez l'obtenir en faisant une requete avec dig, mais par sécurité, je préfère attendre 1 ou 2 jours avant de la supprimer. De même, je vérifie toujours que les signatures via https://dnsviz.net/ sont valides avant de les supprimer.