*** Sur votre serveur AUTORITAIRE ***

1. Allez dans le répertoire où se trouve la zone, et faire une sauvegarde
   de la zone (en supposant que ça s'appelle " mytld "), juste au cas où:

    $ cd /etc/namedb/master
    $ Sudo cp mytld mytld.backup

  Créer un répertoire pour les clés, que nous allons créer:

    $ sudo mkdir /etc/namedb/keys
    $ sudo chown bind /etc/namedb/keys

    $ cd /etc/namedb/keys

2. Générer la première paire de clés (Clé de signature de zone - ZSK)

    $ sudo dnssec-keygen -a RSASHA1 -b 1024 -n ZONE mytld

    Le résultat sera quelque chose comme:

```
Generating key pair.....................+++++
+ ..................................................................................
.........................++++++
Kmytld.+005+51333
```

4. Générer une seconde paire de clés (Clé de signature de clé - KSK)

    $ sudo dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE mytld

    Encore une fois, vous verrez une sortie semblable à ceci:

```
Generating key pair.........................................++
+ ..........................................................................+++
Kmytld.+005+52159
```

  Regardons les clés

```
    # ls -l Kmytld.+005+5*
    -rw-r--r--  1 root  wheel   203 Nov 29 00:07 Kmytld.+005+51333.key
    -rw-------  1 root  wheel   937 Nov 29 00:07 Kmytld.+005+51333.private
    -rw-r--r--  1 root  wheel   247 Nov 29 00:07 Kmytld.+005+52159.key
    -rw-------  1 root  wheel  1125 Nov 29 00:07 Kmytld.+005+52159.private
```

4. Ajouter les clés publiques à la fin du fichier de zone:

    Modifiez le fichier de zone pour " mytld " et ajouter les clés à la fin :

    $ cd /etc/namedb/master

    (éditez le fichier " mytld " ou le nom que vous avez choisi , et
      ajouter les lignes correspondant à vos clés). Pour savoir
            quels sont les fichiers à inclure:

    $ ls -lC1 /etc/namedb/keys/K*key

    (copier les noms de fichiers afin que vous n'ayez pas à les taper

à la main)

```
$ sudo ee mytld

; Clés qui seront publiés dans le jeu d'enregistrements DNSKEY

$include "/etc/namedb/keys/Kmytld.+005+51333.key"     ; ZSK
$include "/etc/namedb/keys/Kmytld.+005+52159.key"     ; KSK
```

Incrémenter le numéro de série.
Sauvegardez et quittez.

5. Signez la zone avec les clés

```
$ cd /etc/namedb/keys
$ sudo dnssec-signzone -o mytld ../master/mytld
```

La sortie devrait ressembler à :

```
Verifying the zone using the following algorithms: RSASHA1.
Zone signing complete:
Algorithm: RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                    ZSKs: 1 active, 0 stand-by, 0 revoked
../master/mytld.signed
```

NOTE : nous n'avons pas besoin de spécifier quelles clés
nous allons utiliser - par défaut dnssec-signzone signera
à l'aide des clés qu'il trouve énumérées dans le zone (celles
que nous avons ajouté via la méthode $include dans l'étape 4).

Si vous voulez spécifier explicitement les clés à utiliser,
vous écririez quelque chose comme (ne le faites pas):

```
$ sudo dnssec-signzone -o mytld -k Kmytld.+005+52159 ../master/mytld Kmytld.
+005+51333
```

La zone signée a été écrite dans le répertoire master/, nous allons donc
l'inspecter:

```
$ cd /etc/namedb/master/
$ ls -l mytld*

-rw-r--r--  1 root  wheel   292 Nov 29 00:08 mytld
-rw-r--r--  1 root  wheel   292 Nov 29 00:10 mytld.backup
-rw-r--r--  1 root  wheel  4294 Nov 29 00:20 mytld.signed
```

Jetez un œil au contenu de la zone, et observez les nouveaux
enregistrements et signatures.

6. Remarquez qu'un jeu d'enregistrements DS a été généré, et est prêt à
être communiquée à la zone parent :

```
$ cd /etc/namedb/keys/
$ ls -l dsset-*

-rw-r--r--  1 root  wheel  155 Nov 29 00:22 dsset-mytld.
```

Regardez le contenu du Dsset :

```
$ cat dsset-mytld.
```

Vous devriez voir deux lignes , une pour chaque algorithme de hachage utilisé pour la KSK .

7. Modifier la définition dans /etc/namedb/named.conf qui charge la zone, et faire charger la la zone signée :

```
$ sudo ee /etc/namedb/named.conf

zone "mytld" {
        type master;
        file "/etc/namedb/master/mytld.signed"; // charger la zone signee
};
```

8. Toujours dans le named.conf , activer DNSSEC (pour la partie autoritaire):

... dans la section options { .. }; ajoutez la ligne suivante

```
dnssec-enable yes;
```

9. Reconfigurer / redémarrer votre serveur de noms

```
$ sudo rndc reconfig
```

Vous pouvez également faire (mais il n'est probablement pas nécessaire):

```
$ sudo rndc reload mytld
```

... pour "forcer" un rechargement de la zone. reconfig devrait normalement le faire, mais ça ne fait pas de mal :)

10. Vérifiez que le serveur de noms répond avec des enregistrements DNSSEC :

```
$ dig @127.0.0.1 mytld SOA +dnssec
```

11. Maintenant, vous devez vous assurer que votre esclave a également configuré leur serveur de noms pour activer DNSSEC dans leur configuration (étape 8). Ils ont dû le faire depuis qu'ils travaillent sur le même laboratoire , mais vérifiez de toute façon !

Pour tester :

```
$ dig @10.10.Y.1 mytld SOA +dnssec
```

... où Y est l'adresse IP du partenaire que vous avez choisi d'être esclave de votre domaine - cela pourrait être l'instructeur, vérifier avec eux .

12. Vous devez maintenant communiquer les DS à votre parent

Demander au gestionnaire de la zone parent sur la façon de communiquer le DS. Ça serait soit avec SCP ou à l'aide d'une interface Web:

a) si vous utilisez le RZM :

Aller à https://rzm.dnssek.org/

Connectez-vous (vous devez vous être inscrit précédemment)

Vérifiez sous Trust Anchor Details que votre DS est
automatiquement est apparu et correspond. Il n'est PAS
automatiquement activé - la seule chose le le RZM a fait est
"saisir" la clé de votre zone et est en attente de votre confirmation
pour l'activation du DS dans la zone parente.

b) si vous n'utilisez pas le RZM :

Si le gestionnaire de la zone parent (racine) dit d'utiliser scp,
procédez comme suit :

```
$ cd /etc/namedb/keys
$ scp dsset-mytld. sysadm@a.root-servers.net:
```

... cela va copier le fichier "dsset-mytld." dans le répertoire
de l'utilisateur "sysadm" sur a.root-server.net, où le gestionnaire
de racine l'inclura dans zone racine afin de le signer.

Prévenez-le gestionnair quand vous avez téléchargé le fichier si vous
utilisez la méthode "scp" .

13. Attendez quelques minutes, jusqu'à ce que vous soyez certain que la
DS est inclus dans la zone parent (root).

Puis, en utilisant dig :

```
dig @a.root-servers.net DS mytld.
```

... alors vous pouvez commencer à tester la validation !

14. Vérifiez que le bit d'AD est positionné :

```
# dig @10.10.0.230 +dnssec www.MYTLD.
```

L'est-il ?

Sinon, notez que le gestionnaire de la racine n'a peut-être
pas encore signé la zone racine avec votre DS inclus dedans.
ou en raison d'un cache TTL négatif, l'enregistrement
DS peut ne pas être dans le cache du résolveur. Vous pourriez
avoir à attendre, mais vérifiez auprès de votre gestionnaire
de racine, et vous pouvez toujours vérifier à la racine :

```
# dig @a.root-servers.net DS mytld.
```

... pour vérifier que la DS est publié . Ensuite, c'est une
question d'attente que le cache expire sur le résolveur, avant
que vous puissiez vérifier votre signatures.

Sinon, ne pas attendre et de procéder à l'activation de la valisation
sur votre resolveur (resolv.grpX.dns.nsrc.org) - voir le laboratoire
concerné !