Rollover with OpenDNSSEC

1. Make sure that your zone is validating correctly.

Things to verify (also if your zone works!)

- look at the key id of your KSK (ods-ksmutil key list -v --zone mytld)

- is BIND loading the right zone ? (compare SOA serial value in /usr/local/var/opendnssec/signed with that returned by dig @auth1.grpX.dns.nsrc.org SOA mytld)

- verify that the right DS is loaded in the root zone

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

- compare the key ID of the DS in the root (output from above) with that of the key used to sign your DNSKEY RR

  ```
  dig @auth1.grpX.dns.nsrc.org DNSKEY mytld +dnssec +multi
  ```

  (look for the key id on the RRSIG)

  If there are any problems problems, correct them.

  Remember to check that the serial on the master is NOT less than the serial on your slave server(s) !

2. Check the key states

```
    # ods-ksmutil key list -v --zone mytld
```

You should have at least one KSK in `active` or `publish` state, and one or more ZSKs (one `active` and possibly others in `retire` or `publish` state).

3. Trigger a ZSK rollover

Since we have very short timers for this lab, rollovers have already been happening on the ZSK! What happens if we decide to do a rollover manually ?

```
    # ods-ksmutil key rollover --zone mytld --keytype ZSK

    Manual key rollover for key type zsk on zone mytld initiated
    Notifying enforcer of new database...

    # tail /var/log/messages
```

You may see a message similar to this:

```
Mar 21 09:38:57 auth1 ods-enforcerd: WARNING: ZSK rollover for zone 'mytld'
not completed as there are no keys in the 'ready' state; ods-enforcerd will
try again when it runs next
```

From the OpenDNSSEC documentation:

OpenDNSSEC makes sure that the zone is secure during the rollover process. This message comes when there is no key that has been published long enough. You probably have no standby keys in your policy. When you initiate the rollover, then OpenDNSSEC first needs to publish the key and after a moment make it active. So do not worry, the rollover process will be finished in a moment.

> The reason you are seeing this is because we are using very short timers in this lab, and keys are not published very long, before they have to be rolled already.

Wait a few seconds, then show the keys again

```
# ods-ksmutil key list -v --zone mytld
```

You should see 3 keys:

- 1 KSK in state 'ready', with a next transition of 'waiting for ds-seen'
- 1 ZSK in state 'active' (the previous ZSK)
- 1 new ZSK in state 'publish'

Effectively, OpenDNSSEC is now rolling ZSKs automatically. It will do this without your help, but you can always trigger a rollover for emergency reasons.

5. Testing a KSK rollover

Take a look at the existing keys:

```
# ods-ksmutil key list -v
```

```
Keys:
Zone:                           Keytype:      State:    Date of next transition
(to):  Size:   Algorithm:  CKA_ID:                           Repository:
Keytag:
mytld                           KSK           active    2014-03-22 09:06:56
(retire)   2048    8          0c4f577032e04e2eb34163382a4524d7  SoftHSM
44096
mytld                           ZSK           active    2014-03-21 11:53:07
(retire)   1024    8          b33d11faf20c649793a0d502fdf15f79  SoftHSM
48718
mytld                           ZSK           publish   2014-03-21 12:01:07 (ready)
1024    8          816e4714df87ffdaddb014481dfcd168  SoftHSM
64656
```

Now, let's issue a rollover. Remember, KSK rollovers can't happen automatically in most cases, so you will need to help OpenDNSSEC by:

- exporting the DS of the new key once you initiate the rollover
  (ods-ksmutil key export --zone mytld --keystate ...)

- telling OpenDNSSEC when you can see that the root/parent has included your DS in their zone
  (ods-ksmutil key ds-seen --zone mytld --keytag XXXXX)

Ok let's rollover:

```
# ods-ksmutil key rollover --keytype KSK --zone mytld
```

Look at the key states:

```
    # ods-ksmutil key list

Keys:
Zone:                           Keytype:      State:    Date of next transition:
phil                            KSK           active    2014-03-21 11:57:18
phil                            KSK           publish   2014-03-21 12:05:19
phil                            ZSK           active    2014-03-21 11:53:07
phil                            ZSK           publish   2014-03-21 12:01:07
```

You should now see that there is an extra KSK
We leave the rest of this exercise up to you :)

6. See what rollovers are automatically planned, and when

```
    # ods-ksmutil rollover list
```