Manual Key Rollover Exercise

OBJECTIVE

We are going to roll the KSK for the zones we have just signed.

REMINDERS

- we are keeping our keys in /etc/namedb/keys/

- we currently have two or more keys in that directory, one KSK and one or more ZSKs.
  Each key is represented by two files, one ending in ".key" (the public key) and one ending in ".private" (the private key)

- there is a DS RRSet in the "root" zone corresponding to our KSK

KSK ROLLOVER

The process is rather similar to the ZSK rollover:

1. Go to the key dir:

```
$ cd /etc/namedb/keys/
$ ls K*
```

2. Just like in step 2 of the ZSK rollover, generate a new KSK
   You will need to use the "-f KSK" parameter to dnssec-keygen:

```
$ sudo dnssec-keygen -f KSK mytld
```

   (Note we don't explicitly set the bitsize - dnssec-keygen defaults to 1024 for ZSKs and 2048 bits for KSKs). Changing the size of the keys is not a problem.

3. Calculate a DS RRSet for the new KSK.

```
$ cd /etc/namedb/keys/
$ sudo dnssec-dsfromkey Kmytld.+005+54511.key > dsset-mytld-54511.
```

  (here 54511 is just the ID of the new KSK so we know which DS is which).

4. Upload the dsset for your zone, using the web interface or using SCP as shown by the root instructor

   Tell an instructor that you have submitted a new DS RRSet, and that you would like it to be added to the "root" zone. If you used the web interface ("RZM"), this should have happened automatically.

5. Double check that the new DS is published in the parent (root) zone alongside the existing one (you should wait at least 2 x TTL until all the caches are updated):

```
$ dig DS mytld
...
;; ANSWER SECTION:
mytld    900 IN  DS 12345 5 2 31F1...
```

```
   mytld    900 IN  DS 54511 5 2 983F...  // <-- the new KSK
   ...
```

   Since both DS are now present in the cache, we can roll our KSK.

   Then we add the new KSK to the zone (edit the file), and we comment
   out (remove) the old KSK:

   From this:

```
$include "/etc/namedb/keys/Kmytld.+005+46516.key"; // KSK
```

   To this:

```
;$include "/etc/namedb/keys/Kmytld.+005+46516.key"; // KSK old
$include "/etc/namedb/keys/Kmytld.+005+54511.key"; // KSK new
```

    Remember to increment the serial number too.

    ... notice how we simply get rid of the old KSK - we don't need
    it - both DS records are there, so it's enough to have only one
    KSK, since we already "know" about its DS "on the internet".

6. Let's sign the zone with the new KSK

```
  $ cd /etc/namedb/keys
  $ sudo dnssec-signzone -o mytld -k Kmytld.+005+54511 ../master/mytld Kmytld.
+005+45000

  $ sudo rndc reload mytld
```

7. Check with dig - both before and after the TTL expire (or cache flush)

```
  $ dig dnskey mytld
  $ dig dnskey mytld +dnssec
```

8. Tell an instructor that you would like the original DS resource
   records to be removed from the "root" zone (or remove it yourself
   using the web interface, if using the "RZM")

9. Sit back and reflect on what an involved and annoying process
this was, and how much better things would be if all your key
rollovers were managed automatically.