Manual Key Rollover Exercise

OBJECTIVE

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

REMINDERS

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

- we currently have two keys in that directory, one ZSK and one KSK. 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

ZSK ROLLOVER

1. Take a look at what keys we have already generated. Make a note of the names of the files containing the current ZSK and KSK.

```
# cd /etc/namedb/keys/
# ls
```

2. Generate a new ZSK, which we will use to replace the old one.

```
# dnssec-keygen mytld    <---- replace mytld with the name of your zone
```

Make sure all the keyfiles are readable by the named process:

```
# chgrp bind K*
# chmod g+rw K*
# ls
```

You should now have a third key pair in the directory. If you check the DNSKEY RDATA, you should see the flags field is 256 (i.e. this is a ZSK, not a KSK). Make a note of the name of the file containing the new ZSK.

3. Take a look at your current DNSKEY RRSet.

```
# dig mytld dnskey
```

Your zone should contain one KSK and one ZSK (check the flags to distinguish between them).

4. Re-sign your zone to include signatures by the new ZSK.

```
# rndc sign mytld
# tail /etc/namedb/log/general
```

5. See what difference this has made to the zone.

```
# dig mytld dnskey
# dig mytld dnskey +dnssec
# dig mytld soa +dnssec
```

Your zone should now contain one KSK and two ZSKs; both ZSKs should be

present in the DNSKEY RRSet, which should be signed by the KSK. The SOA record (and other RRSets in the zone) should now be signed twice, once by each ZSK, and you should see corresponding pairs of RRSIGs.

6. Retire the old ZSK.

```
# cd /etc/namedb/keys/
# dnssec-settime -D +1 <old ZSK name>
# chgrp bind K*
# chmod g+rw K*
# rndc sign mytld
# tail /etc/namedb/log/general
```

The old keys will remain in the directory, but contain a Delete field near the top of the file indicating when they should no longer be used. Note that BIND will not remove keys immediately if signature expiration timers and TTLs suggest this might be unsafe.

We specified a destroy time of now plus one second, which is definitely unsafe. This means in effect that the old ZSK will be retired by BIND just as soon as it is safe to do so.

KSK ROLLOVER

7. Repeat steps 1 to 5, except this time replace the KSK. You will need to use the "-f KSK" parameter to dnssec-keygen when you repeat step 2.

8. Calculate a DS RRSet for the new KSK.

```
# cd /etc/namedb/keys/
# dnssec-dsfromkey <filename> >dsset-mytld.
```

9. Upload the dsset for your zone.

```
# scp dsset-mytld. sysadm@rootserv.dns.nsrc.org:
```

The password for rootserv.dns.nsrc.org is the class password.

10. Tell an instructor that you have submitted a new DS RRSet, and that you would like it to be added to the "root" zone.

11. Once you have received confirmation (and you have checked yourself!) that the new DS resource records have been added to the "root" zone, retire the old KSK just as we did with the ZSK in step 6.

```
# cd /etc/namedb/keys/
# dnssec-settime -D +1 <old KSK name>
# chgrp bind K*
# chmod g+rw K*
# rndc sign mytld
# tail /etc/namedb/log/general
```

12. Check back later in the day and verify that the old ZSK and KSKs no longer appear in your zone.

13. Tell an instructor that you would like the original DS resource records to be removed from the "root" zone.

14. 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.