Key States

Most of the key states are as described in the DNSSEC key timing draft: http://tools.ietf.org/html/draft-morris-dnsop-dnssec-key-timing-02

Also see: http://tools.ietf.org/html/draft-mekking-dnsop-dnssec-key-timing-bis-02

The diagram below shows the states described in this draft.

Below is a brief describe of what the states mean:

Generate
Keys in the generate state have been created and stored but not used yet.

Publish
Keys in the publish state have been published in the zone, but are not yet considered safe to use. (i.e. They have not been in the zone long enough to have propagated through the system.)

Ready
Keys in the ready state have been published long enough that we could safely start to use them.

Active
Keys in the active state are those that are in use.

Retired
Keys in the retire state have been in use but have been replaced by a successor, they are post-published while signatures generated with them might still be in the system.

Dead
Keys in the dead state have been retired long enough for them to be safely removed from the zone.

Standby KSK states

The standby keys are experimental. We are currently not supporting offline HSM, which is needed to get the security level needed to fulfill the idea behind standby keys. Will be fixed in a future version.

For standby KSKs there are some extra states which replace Published and Ready. This is because the standby keys are not introduced into the zone until they are needed. Instead their DS record is submitted to the parent - see Uploading a Trust Anchor. (The idea is that if the key is needed in an emergency the shortest timescale that it can be used in is the publication through the child system.)

DSSUB

The DS has possibly been submitted (if it happened automatically) but in any case we are waiting for the ds-seen command.

DS PUBLISH

The ds-seen command has been given, and we are now waiting for the various propagation delays and safety margins to pass.

DSREADY

The DS record is now considered safe to use, so the standby key is ready.

KEY PUBLISH

We have been asked to use the standby key so we have published it in the zone. Once the key has propagated through the system it will move into the active state.