tldbox GmbH
Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria
T +43 662 46 69 -730
office@tldbox.at · **www.tldbox.at**

Our well-established model for the KSK rollover processes is as follows:

Setup and Onboarding:

As the MAIN RSP, we assume the central role in coordinating the KSK rollover between the involved parties (DNSSEC-RSP, Registry Operator, IANA). Communication methods (email, phone) are requested during the customer / DNSSEC-RSP onboarding, and added to our operational documentation. These include emergency communication means (typically mobile phone numbers). However, we also believe that the scheduling of actual KSK rollovers is the responsibility of the DNSSEC-RSP, as they would understand the operational requirements based on their signing infrastructure & policies. We will, however, ask the DNSSEC-RSP for their rough schedule of rollovers, so that we can plan and prepare ressources accordingly.

We assume that our contact information is used as technical contact in the IANA RZM, while the Registry Operator's contact information is used as the administrative contact. Other models might be possible on customer demand,

Process for non-emergency KSK rollover

The non-emergency KSK rollover is assumed to be executed at regular intervals, and "pre planned" by DNSSEC-RSP and MAIN-RSP. In the ttached flow we shows our proposal of the basic steps for for a successful KSK rollower, and we demonstrate the responsibility of each involved party. The proposed process might change depending on specific requirements of the DNSSEC-RSP (or the Registry Operator). We propose a single-step DS change in the root zone, but customers/DNSSEC-RSPs might have a different preference, to which we would adopt. Details of the process steps are described below:

- KSK rollover announcement (by DNSSEC-RSP): DNSSEC-RSP informs us about the planned KSK rollover.
- We confirm the planned KSK rollover (these two steps also automatically double-check the availability of two-way communication between DNSSEC and MAIN RSP), and plan resources on our side. At the same time, the Registry Operator confirms this change with the DNSSEC-RSP (practically, in a short 3-party call/video conference of all involved parties).
- At the planned date/time, the DNSSEC RSP starts their rollover process, and we are on stand-by in terms of communication.
- (... more steps on side of DNSSEC-RSP ...)
- Subsequently, The DNSSEC-RSP communicates the new DS record, as well as the DS record to be removed to us, and we confirm the reception of said DNSSEC change.

- We double-check that the new KSK is a) indeed present in the public zone, and b) used to sign the ZSKs (even though we understand that IANA will perform an identical technical check)
- We submit the change of DS record via the RZM, and wait for IANA's technical check to pass successfully.
- On receiving the technical confirmation request from IANA, we compare the IANA information to our records, and confirm the request unless we find inconsistencies. We might remind the Registry Operator if they don't perform the parallel admin-c confirmation of the change.
- Once the RZM change is complete, we inform the DNSSEC-RSP for them to conitinue their rollover process (see flowchart for our idea of their processes)
- (... more steps by DNSSEC RSP)
- Once the DNSSEC RSP has successfully concluded their process (removal of old KSK etc.) we expect to be contacted, so that we can close the KSK rollover process on our side.

Process for emergency KSK rollover

For the emergency rollover, we propose that an offline emergency key is pre-published in the root zone, so that the time critical interaction with IANA is not required. As this allows the DNSSEC-RSP to fully act on their own in changing signatures in the zone, we assume that an emergency rollover can be performed independently, but we require the DNSSEC-RSP to contact our emergency contact information in such case, so that we our 24/7 operations department can assist if required. We assume that the DNSSEC-RSP also contacts the Registry Operator directly in that case.

Note that we are open to other emergency processes, and will discuss with the DNSSEC-RSP if such processes are proposed.

Also note that we assume that the ZSK rollover is performed entirely on the DNSSEC-RSPs side, and no communication is required for such rollovers, except in emergency situations.