

DNSSEC.4.14. KSK Rollovers

TLDR strictly adheres to RFC 6781 and RFC 7583 for Key Signing Key (KSK) rollovers, coordinating closely with IANA (Root Zone Operator). The processes and procedures to ensure a successful KSK rollover, including coordination with the MAIN RSP and IANA, are detailed below.

1. Non-Emergency (Planned) Rollover

We employ the "Double-DS" (or Double-Signature) rollover method. When TLDR operates as the DNSSEC RSP and the MAIN RSP is an external party, the following coordination model applies:

- **Step 1 (Preparation & TTL Reduction):** A formal change window is agreed upon in advance. Lowering TTL values is effective only if performed prior to the rollover event. Therefore, pre-rollover TTL reduction for DNSKEY and DS records is coordinated between the DNSSEC RSP and the MAIN RSP several days in advance to ensure faster cache expiration during the transition window.
- **Step 2 (Key Generation):** Generate the new KSK securely in the HSM.
- **Step 3 (Publication):** Publish the new DNSKEY so both old and new keys are present in the zone, and validate the publication.
- **Step 4 (IANA Coordination):** DS submission to IANA via the Root Zone Management System (RZMS) is coordinated with the Registry Operator (if separate).
- **Step 5 (Synchronization):** Serial increments and zone publication are synchronized between the relevant parties. We wait for the DS record to appear in the Root Zone and allow for TTL expiration.
- **Step 6 (Activation & Cleanup):** Mark the new key as "Active" for signing and remove the old key. Post-publication monitoring is conducted to confirm resolver validation globally.

Communication Channels for Planned Rollovers: Coordination is maintained via designated operational contacts, a 24/7 NOC contact list, a ticketing system with change tracking, and an emergency escalation bridge if required.

2. Emergency Rollover

In the event of a confirmed KSK compromise, the "Emergency Revocation" procedure defined in our DPS is triggered. For emergency rollovers, TTL reduction cannot immediately affect

already cached records in recursive resolvers. While TTL values may be lowered for future caching behavior, recovery primarily depends on DS update timing and resolver cache expiry. Mitigation relies on the following steps:

- **Step 1 (Incident Declaration & Notification):** The incident is declared by the DNSSEC RSP SOC. Immediate notification is sent to the Registry Operator and the MAIN RSP operational contact, followed by a joint decision to initiate the emergency rollover. All emergency communication occurs via predefined 24/7 emergency contact channels and documented incident response procedures.
- **Step 2 (Key Generation & Signing):** Immediate generation of a new KSK occurs in the HSM. We use the RFC 6781 double-DS method where feasible. If zone management is controlled by the MAIN RSP, the MAIN RSP ensures zone serial increment and publication, while the DNSSEC RSP generates the new KSK and signs the updated zone.
- **Step 3 (IANA Expedited Submission):** The Registry Operator (as contract holder) coordinates the submission of the new DS record to IANA via expedited Root Zone Management procedures.
- **Step 4 (Revocation & Monitoring):** Where applicable, the RFC 5011 revocation bit is used to signal key invalidation to validating resolvers. The DNSSEC RSP performs continuous monitoring of DNSKEY and DS propagation via multiple global vantage points, providing status updates until global validation stabilizes.

3. Dual Role Clarification

Operational coordination varies based on TLDTR's specific roles for the gTLD:

- **If TLDTR operates both as MAIN RSP and DNSSEC RSP:** Coordination is completely internal. Change management follows documented ISMS change control procedures. IANA communication is handled by the Registry Operator, with technical artifacts prepared by our DNSSEC team.
- **If TLDTR acts solely as DNSSEC RSP:** The external MAIN RSP retains authoritative zone control. TLDTR (as DNSSEC RSP) handles key management and signing. The Registry Operator retains responsibility for DS submission to IANA.