

Additional clarification on KSK rollover roles and coordination (MAIN.1.16)

This section provides additional clarification regarding the division of responsibilities and coordination activities during KSK rollovers, covering both scenarios where TLDTR acts as the DNSSEC RSP and where an external DNSSEC RSP is engaged.

1. TLDTR acting as both MAIN RSP and DNSSEC RSP

When TLDTR provides DNSSEC services directly, the organization assumes end-to-end responsibility for KSK lifecycle management, while maintaining clear separation of duties internally.

Planned (non-emergency) KSK rollover

- The MAIN RSP function initiates the rollover schedule and coordinates timing with the Registry Operator.
- The DNSSEC RSP function within TLDTR generates the new KSK within Cloud HSM, following internal key ceremony and quorum approval procedures.
- The DNSSEC RSP submits the new DS record to IANA Root Zone Management and monitors publication.
- The MAIN RSP verifies DNS resolution and chain-of-trust continuity post-publication and authorizes retirement of the old KSK.

Emergency KSK rollover

- The Security Operations Center (SOC), operating under the MAIN RSP function, declares a DNSSEC security incident.
- A replacement KSK is immediately generated within Cloud KMS. To maintain the chain of trust and prevent the zone from becoming bogus (per RFC 6781), the DNSSEC RSP function ensures both the affected (old) KSK and the new KSK sign the **DNSKEY** RRset.
- An emergency DS submission for the new KSK is coordinated with IANA using established emergency channels.
- Once the new DS record is published at the root, the old DS is removed. Only after the old DS is completely flushed from global resolver caches (accounting for TTL expiration) does the DNSSEC RSP function safely disable and revoke the affected KSK within Cloud KMS under multi-party approval.
- The MAIN RSP oversees validation, registrar notification, and post-incident review.

In this scenario, all communication with IANA is performed by TLDTR in its DNSSEC RSP role, with internal escalation and approval managed under MAIN RSP governance.

2. TLDTR acting as MAIN RSP with an external DNSSEC RSP

TLDTR is designed to support Registry Operators that elect to use an external DNSSEC RSP. In this model, TLDTR retains orchestration and governance responsibility as MAIN RSP, while cryptographic operations are performed by the external DNSSEC RSP.

Planned (non-emergency) KSK rollover

- The MAIN RSP coordinates rollover planning with the Registry Operator and the external DNSSEC RSP.

- The external DNSSEC RSP performs KSK generation, signing operations, and DS preparation according to its certified procedures.
- The external DNSSEC RSP submits the DS record to IANA or provides it to the Registry Operator for submission, depending on contractual arrangements.
- The MAIN RSP tracks execution milestones, validates successful DS publication, and confirms DNSSEC continuity across registry services.

Emergency KSK rollover

- The MAIN RSP initiates incident escalation and acts as the single coordination point.
- The external DNSSEC RSP executes emergency key replacement in accordance with its emergency procedures. Crucially, the external RSP is required to retain the compromised KSK to co-sign the zone until the new DS record is established and the old DS is safely removed from the root zone, ensuring continuous zone validation.
- The MAIN RSP ensures that IANA emergency communication is initiated by the appropriate party and that all actions are tracked, logged, and confirmed.
- The MAIN RSP validates resolution, coordinates registrar notifications, and documents the incident.

3. Coordination and communication with IANA

Regardless of whether TLDTR operates as DNSSEC RSP or interacts with an external DNSSEC RSP, the following principles apply:

- All DS submissions and rollovers are conducted in accordance with IANA Root Zone Management procedures.
- The responsible DNSSEC RSP performs DS generation and submission.
- The MAIN RSP maintains oversight, validation, and auditability of the process, ensuring continuity of service and compliance with ICANN contractual obligations.
- Emergency rollovers utilize IANA-defined emergency communication channels, with clear role assignment and documented authorization.

This dual-model approach ensures that TLDTR can safely support gTLDs using either integrated or external DNSSEC RSP services while maintaining consistent governance, transparency, and DNSSEC chain-of-trust integrity.