The applicant maintains comprehensive operational procedures for both planned and emergency Key Signing Key (KSK) rollovers to ensure the integrity of the DNSSEC trust chain.

Rollover Strategies and Cadence

Defined Roles

- DNS Operations Team: Responsible for implementing key and signing changes on authoritative DNS servers, updating zone configurations, and monitoring propagation and validation status.
- Security Audit Team: Responsible for independent verification of all steps, log integrity review, and issuing a compliance report upon completion.
- External Liaison: Responsible for communication with ICANN/IANA and the .alibaba Registry Operator (RO) regarding DS record submission and removal.

1. Planned KSK Rollover

This KSK rollover follows the Double-Signature model (as per RFC 6781 §4.1.2), where the new and old KSKs simultaneously sign the DNSKEY RRset to ensure continuous validation during transition, with clearly defined roles and TTL-based timing to maintain global DNSSEC integrity. Note our planned KSK rollovers are scheduled every 3 years.

KSK Rollover Timeline and Task Breakdown

For clarity, we define T_0 as the reference start time. TTL_{DNSSEC} and TTL_{DS} are defined as the TTL of DNSKEY and TTL of DS (DS record in the root zone) respectively.

Table 1. KSK Rollover timeline

Phase	Time(duration)	Key Roles and Tasks
initial	1 day before T_0	• DNS Operations Team: Generate the new KSK in the HSM. • Security Audit Team: Confirm secure generation and storage of new KSK • DNSKEY RRset: old KSK+old ZSK
new DNSKEY	Start at T_0 Duration: 2* TTL_{DNSSEC}	• DNS Operations Team : Add the new KSK to the DNSKEY RRset, sign the DNSKEY RRset with both old and new KSKs and publish the updated zone. • Security Audit Team: Verify the updated zone by DNS queries. Setup recursive resolvers to validate cache content. • External Liaison: Inform ICANN/IANA/RO the start of new DNSKEY phase. • DNSKEY RRset: old KSK+old ZSK+new KSK

		Note: the new DNSKEY phase will last at least TTL_{DNSSEC} to make sure that the old DNSKEY RR has expired from caches. We will wait twice TTL_{DNSSEC} before move to next phase.
DS change	Start after **new DNSKEY** phase Duration: +2* TTL_{DS}	• External Liaison: Provide the new KSK or new DS to IANA via Root Zone Management (RZM) system. Request ICANN/IANA to replace old DS with new DS. (via RO) • DNS Operations Team : Monitor and confirm a new DS RR has been published that points to the new KSK. Confirm resolvers can validate new KSK using new DS. • Security Audit Team: Validate complete chain of trust (root → .alibaba → test.alibaba) • DNSKEY RRset: old KSK+old ZSK+new KSK Note: After the new DS has been published and propagated, DNSSEC RSP should wait at least TTL_{DS} to make sure that the old DS RR has expired from caches. We will wait twice TTL_{DS} before moving to next phase.
DNSKEY removal	Start after **DS change** phase	• DNS Operations Team : Remove old DNSKEY from zone file re-sign and publish a new zone. • Security Audit Team: Validate that the zone is updated as planned. Validate complete chain of trust (root → .alibaba → test.alibaba). Issue a compliance report upon completion • DNSKEY RRset: old ZSK+new KSK

2. Planned ZSK Rollover

This ZSK rollover utilizes the Pre-Publish method (as per RFC 6781 §4.1.1.1)，where the new ZSK is first published in the DNSKEY RRset and allowed to propagate before being used to sign zone data, and the old ZSK is only removed after all its signatures have expired from caches, ensuring uninterrupted DNSSEC validation. Note the planned ZSK rollovers are performed every 3 months.

ZSK Rollover Timeline and Task Breakdown

Firstly, we define T_0 as the start time. TTL_{DNSSEC} and $TTL_{zone\text{-}max}$ are defined as the TTL of DNSKEY and the maximum TTL of other records in the zone, respectively.

Table 2. ZSK Rollover timeline

Phase	Time(duration)	Key Roles and Tasks
initial	1 day before T_0	• DNS Operations Team: Generate the new ZSK in the HSM. • Security Audit Team: Confirm secure generation and storage of new ZSK • DNSKEY RRset: old KSK+old ZSK

new DNSKEY	Start at T_0 Duration: 2* TTL_{DNSSEC}	• DNS Operations Team : Add the new ZSK to the DNSKEY RRset and continue sign the zone using the old ZSK . The KSK signs the updated DNSKEY RRset. Publish the zone. • Security Audit Team: Confirm the new ZSK is present in DNSKEY RRset and KSK-signed RRSIG over DNSKEY is valid. Setup recursive resolvers to validate cache content. • DNSKEY RRset: old KSK+old ZSK+new ZSK Note: the new DNSKEY phase will last at least TTL_{DNSSEC} to make sure that the old DNSKEY RR has expired from caches. We will wait twice TTL_{DNSSEC} before move to next phase.
new RRSIGs	Start after **new DNSKEY** phase Duration: +2* $TTL_{zone\text{-}max}$	• DNS Operations Team : Start signing zone data with the new ZSK and stop signing the data with the old ZSK. Monitoring the propagation and validation status. • Security Audit Team: Confirm zone RRsets are only signed by the new ZSK. Validate end-to-end DNSSEC chain • DNSKEY RRset: old KSK+old ZSK+new ZSK Note: After the new signature has been published and propagated, DNSSEC RSP should wait at least $TTL_{zone\text{-}max}$ to make sure that the old DNSKEY RR has expired from caches. We will wait twice $TTL_{zone\text{-}max}$ before moving to next phase.
DNSKEY removal	Start after **new RRSIGs** phase	• DNS Operations Team : Remove old DNSKEY from zone file ,re-sign and publish a new zone. • Security Audit Team: Confirm old ZSK is no longer in DNSKEY RRset. Final validation of zone integrity. Issue a compliance report upon completion. • DNSKEY RRset: old KSK +new ZSK •

Note for both KSK and ZSK rollover process, a strict rollback mechanism is in place: if any validation failure, operational anomaly, or monitoring alert occurs at any phase, the procedure is immediately halted and reverted to the previous stable state. For example, if DNSSEC validation issues are detected during the DNSKEY removal phase, the DNS Operations Team will promptly re-add the retired key to the DNSKEY RRset and re-enable dual-signing with both the old and new keys.

3. Emergency KSK Rollover

In the event of a suspected or confirmed key compromise, we initiate an expedited rollover. This involves the immediate generation of a new KSK and an out-of-band

notification to the Main Registry Operator (RO) to trigger an urgent DS update via IANA.

Practice and Readiness Drills

To ensure operational readiness and minimize the risk of human error, the applicant conducts the following practice activities:

- Annual Operational Drills: At least once a year, our technical team performs a full-cycle KSK rollover in a dedicated Sandbox/Pre-production environment. This environment mirrors the production signing infrastructure. The drill tests the generation of keys, the signing of the RRset, and the generation of the DS record.
- Emergency Response Tabletop Exercises: We conduct semi-annual tabletop exercises specifically for "Emergency KSK Rollovers." These exercises simulate high-pressure scenarios (e.g., HSM failure or key compromise). We walk through the escalation path, internal communication protocols, and the secure transfer of DS records to the Main RSP.
- Documentation Review and Update: Following each drill or exercise, an "After-Action Report" (AAR) is generated. We review any bottlenecks or points of confusion and update our Standard Operating Procedures (SOPs) accordingly to ensure they remain accurate and effective.
- Staff Training: All DNSSEC operators undergo mandatory training on the DNSSEC signing platform and the specific coordination requirements with the Main RO and IANA.

IANA Coordination and Role Clarification

The applicant acknowledges its role as the Third-Party DNSSEC RSP. The Main Registry Operator (RO) remains the entity responsible for formal communication with IANA. Our coordination chain is strictly defined:

- Third-Party DNSSEC RSP (Applicant): Generates new KSK/DS records and monitors TTL/propagation timings.
- Secure Transfer: We transfer the new DS record to the Main RSP’s designated security contact via a pre-agreed, encrypted, and authenticated channel (e.g., PGP-encrypted email or secure portal).
- Main RSP -> IANA: The Main RSP submits the update to IANA via the Root Zone Management System (RZMS).

If the applicant serves as both the Main RSP and the DNSSEC RSP, the internal workflow between the DNS team and the IANA liaison team is integrated into a single automated or manual ticketing process to ensure seamless DS updates.