As the MAIN RSP, ZDNS deeply understands that its core role in the KSK Rollover process is that of a coordinator and guarantor. We are responsible for coordinating the changes of DNSKEY and DS records safely, accurately and timely between DNSSEC RSP and IANA. To ensure the safe and successful completion of the KSK rollover, we have developed detailed and test-validated standard KSK rollover procedures for both planned and emergency situations.

The following are the processes and procedures we adopt to ensure a successful KSK Rollover.

Non-Emergency (Planned) Rollover Process

Per the stipulations in ZDNS's KSK Rollover Specifications, ZDNS's technical platform is required to perform a KSK rollover once a year. Each KSK rollover shall be strictly executed in accordance with the KSK Rollover Process, and the entire execution process involves the collaboration of ZDNS, DNSSEC RSP, Registry Administrators, and IANA.

ZDNS mainly adopts the Double-KSK Method for conducting KSK rollovers. ZDNS has developed a KSK Rollover Process to guide and implement the entire KSK rollover process. The entire rollover process is mainly divided into four phases, and the following sections present the definition of ZDNS's KSK Rollover Process.

Phase 1: Preparation and Key Generation

Initiation

In accordance with the KSK Rollover Specifications, ZDNS initiates the key rollover plan in the 4th quarter of each year. Based on the predefined key lifecycle policy, our Key Management Specialists formulate the KSK Rollover

plan at the appropriate time and launch the rollover process as scheduled. After internal approval, a written KSK rollover notification is issued to all relevant parties, including Registry Administrators and the DNSSEC RSP side. During the initiation phase, we reserve a one-week period for relevant parties to collect and provide feedback.

New Key Generation

After our internal Security Team coordinates with the DNSSEC RSP, the DNSSEC RSP generates the new key as planned.

Secure Transmission

After generating the new key, the DNSSEC RSP transmits the corresponding DS records to ZDNS through a mutually authenticated secure channel.

Phase 2: Pre-Release Phase

Official Pre-Release

After all relevant parties have no further comments, ZDNS issues an official notification to the DNSSEC RSP, requesting it to publish the new KSK records into the Zone File and perform the rollover in accordance with the established rollover plan.

Verification and Monitoring

After the DNSSEC RSP confirms execution, the automated monitoring systems of both ZDNS and the DNSSEC RSP will continuously verify whether

the new KSK records are correctly included in the online zone data, and compare and verify them against the expected values. We maintain this propagation period for several weeks to ensure that the vast majority of recursive resolvers worldwide have cached the new KSK records.

Phase 3: Coordination with IANA (Root Zone Update)

Submission of Official Request

After the propagation period ends, ZDNS submits a DS record change request and provides the new DS records via the official channel of IANA's RZM system. This operation requires multi-factor authentication.

Tracking and Confirmation

ZDNS closely tracks the status of the IANA ticket. Meanwhile, ZDNS's monitoring system proactively queries the root servers to confirm that the DS records in the Root Zone have been successfully updated.

Phase 4: Completion and Old Key Deletion

KSK Activation

After the Root Zone DS records take effect, the DNSSEC RSP sets the new KSK to the active state.

Removal of Old DS Records

After confirming the Root Zone update and undergoing a waiting period (to ensure global cache invalidation), ZDNS will instruct the DNSSEC RSP to completely remove the old KSK records from the Zone File. At the same time, ZDNS will submit a request for deleting the old DS records in the RZM system.

Archiving or Destruction of Old Key

The private key of the old KSK will be securely archived or completely destroyed in accordance with our key lifecycle policy.

Emergency Rollover Process

The emergency rollover process for ZDNS KSK is triggered by suspected or confirmed key security incidents. This process compresses the timeline and prioritizes security over smooth transition.

Phase 1: Immediate Incident Response

Activation of Emergency Team

Once signs of a key security risk incident are detected by our Intrusion Detection System (IDS) or Hardware Security Module (HSM) alerts, our 24/7 Security Incident Response Team (SIRT) is activated immediately.

Authorization and Declaration

The SIRT lead holds pre-authorization to bypass the regular change approval process and directly declare the activation of the emergency rollover plan.

Phase 2: Emergency Coordination with DNSSEC RSP

Out-of-Band Communication

We immediately contact the designated security lead of DNSSEC RSP via the pre-established emergency security phone hotline, declare the entry into emergency status, and activate the emergency protocol.

Synchronized Instructions

We require DNSSEC RSP to immediately generate a new KSK, and generate and publish the KSK record for a new emergency KSK (KSK-emergency) into the Zone File. This is a rapid, one-step operation aimed at cutting off the old key and establishing new trust in the shortest possible time. Meanwhile:

1. Reduce the TTL (Time-to-Live) of the DNSKEY to enable the DNSKEY RRset (Resource Record Set) to expire faster from the cache;
2. Shorten the signature validity period.

Phase 3: Emergency Coordination with IANA

After the DNSSEC RSP completes the publication of the new key, it submits a DS record change request in the IANA RZM system and provides the new DS records.

Meanwhile, ZDNS will simultaneously respond via an emergency email: it sends a DS change request marked as "SECURITY EMERGENCY" to ICANN and IANA, enclosing the new DS records and a brief description of the incident.

Subsequently, we will immediately call the IANA emergency contact number documented in our operational manual, verbally notify the other party of the

occurrence of a critical security incident, inform them of the submitted ticket number, and request that they handle it with the highest priority.

Proactive Follow-Up

Our IANA Liaison Specialist will proactively and continuously maintain communication with IANA until the Root Zone update is completed, and stand ready to provide all required information at any time.

Deletion of the Old KSK

After confirming that the new DS records in the Root Zone have taken effect, the old KSK is deleted immediately.

Phase 4: Post-Incident Review

After the incident is stabilized, we will conduct a thorough Root Cause Analysis (RCA) and Post-mortem.

Subsequently, we will initiate a standard, planned KSK rollover process to replace the emergency-generated KSK-emergency, bringing it back into normal key lifecycle management.

Coordination Mechanisms

Coordination with DNSSEC RSP

1. Guarantees via Contracts and SLA

The service contract between ZDNS and DNSSEC RSP clearly stipulates the latter’s responsibilities in KSK rollover, response time SLAs (especially in emergency scenarios), and communication protocols.

2. Secure Communication Channels

We have established strongly authenticated APIs for routine command and data transmission, as well as out-of-band communication (secure phone calls, encrypted emails) for emergency situations—ensuring that command channels are never interrupted.

3. Joint Drills

ZDNS conducts at least one joint tabletop exercise with DNSSEC RSP each year, simulating both planned and emergency rollover scenarios to test processes, familiarize all parties with procedures, and optimize collaboration.

Coordination and Communication with IANA

1. Adherence to Official Channels

All DS record change requests are strictly submitted via the official channel of the IANA RZM system, ensuring the authority, security, and auditability of operations.

2. Maintenance of Emergency Contact Lists

ZDNS and IANA mutually confirm and regularly update the 24/7 emergency security contact list.

3. Maintaining Transparency and Proactivity

In all communications—especially in emergencies—ZDNS maintains a high level of transparency with IANA, proactively providing all necessary information in a clear manner to enable IANA to quickly assess the situation and execute operations.

In summary, during its tenure as the MAIN RSP, ZDNS will serve as a reliable, efficient, and secure coordination hub in the DNSSEC trust chain. Through rigorous processes, automated monitoring, regular drills, and clear,

transparent communication, ZDNS ensures the successful completion of KSK Rollover under all circumstances, safeguarding the resolution security and stability of top-level domains (TLDs).