DNSSEC.4. DNSSEC Capabilities

As the DNSSEC RSP, we shall strictly comply with the RFC 6781 standard and the requirements of our DPS, conducting KSK rollovers for each of the gTLDs we operate at least once annually, and maintaining close collaboration with the Main RSP throughout the entire process. We have clearly defined the job responsibilities and task execution requirements for each phase of the full KSK rollover process within our organization, with all procedures fully aligned with the RFC 6781 standard. The internal role allocation and detailed task execution timeline for the full process are as follows:

1. Job Responsibilities for KSK Rollover

1）DNS Operations Engineer (HSM Operator)

Responsible for submitting the application for the annual KSK key rollover work plan.

Configuring the DNSSEC signing system and implementing the dual-signature strategy in accordance with RFC 6781 requirements.

Generating and verifying the format and validity of DS records corresponding to the new KSK public key.

Monitoring the operational status of the signing system 24/7, verifying the integrity of the DNSSEC trust chain during the rollover transition period, and promptly resolving technical faults.

2）DNS Technical Coordinator (HSM Administrator)

As the primary point of contact with the Main RSP, responsible for establishing and maintaining real-time communication channels to ensure external coordination for the entire rollover process.

Organizing internal coordination meetings, tracking the progress of each phase, and documenting the timeline.

3）Principal of Network Operations Center (Management Decision-Maker)

Approving the annual KSK key rollover work application.

Holding the hardware HSM key storage card and providing the personally held key share for authentication when participating in key operations.

4）Internal Audit Administrator

Conducting full-process security reviews of all stages of the key rollover (key generation, transmission, deployment, revocation).

Verifying the compliance of operational procedures and internal security policies.

2. Regular Annual KSK Rollover Process

1）Pre-Rollover Preparation and Confirmation

This phase primarily involves determining the rollover plan, completing internal resource preparation, and confirming the rollover time window and collaboration rules with the Main RSP. The tasks executed internally during this phase are as follows:

DNS Operations Engineer (HSM Operator): Checks the availability of the HSM and key generation tools, completes the full offline backup of the old KSK; drafts the annual KSK key rollover work plan (including the detailed rollover timeline, task list, and key generation

specifications) and initiates an internal application.

DNS Technical Coordinator (HSM Administrator): Conducts the initial collaboration with the Main RSP via official email and video conference to confirm communication channels, submission requirements (DS record format, encrypted transmission method), and the rollover time window.

Principal of Network Operations Center (Management Decision-Maker): Approves the annual KSK key rollover work plan.

Internal Audit Administrator: Conducts a security review of the pre-roolover preparation work.

2) Generation of New KSK and Corresponding DS Records
The tasks executed internally during this phase are as follows:
DNS Operations Engineer (HSM Operator): Generates a new KSK key pair and the corresponding DS record, and verifies the consistency between the public key and the DS record.

DNS Technical Coordinator (HSM Administrator): Verify the consistency between the public key and the DS record; synchronizes the key generation progress with the Main RSP to prepare for subsequent submission.

Internal Audit Administrator: Monitors the entire key generation process to ensure compliance.

3) Enabling the Dual-Signature Strategy (Old KSK + New KSK) and Submitting DS Records to Avoid Trust Chain Interruption
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Configures the DNSSEC system to enable the dual-signature strategy of old KSK + new KSK, verifies the zone file signature logs to confirm the effectiveness of the dual-signature.

DNS Technical Coordinator (HSM Administrator): Submits the new KSK public key and DS record through the encrypted channel agreed with the Main RSP; confirms successful receipt by the Main RSP, synchronizes the status of the enabled dual-signature strategy, and urges the Main RSP to proceed with deployment and resolution loading.

Internal Audit Administrator: Monitors the key transmission process to ensure compliance.

4) Continuous Verification of the Validity of the DNSSEC Trust Chain During the Rollover Transition Period
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Monitors the operation of the DNSSEC signing

system; deploys monitoring system indicators to track the deployment and resolution loading status of the Main RSP, global resolution coverage, and the validity of the DNSSEC trust chain.

DNS Technical Coordinator (HSM Administrator): Synchronizes progress with the Main RSP via the collaboration group, records feedback from the Main RSP, confirms that the Main RSP has completed the submission and deployment of the new DS record in the IANA root zone system, obtains confirmation of the successful global deployment by the Main RSP, and reports the progress to the Principal of Network Operations Center.

5) Revoking the Old KSK and Restoring the New KSK Single-Signature Strategy After the New DS Record Takes Effect Globally

The tasks executed during this phase are as follows:

DNS Operations Engineer (HSM Operator): After obtaining approval, marks the old KSK as inactive and stops its use for signing, switches to the new KSK single-signature strategy, verifies the signature logs to confirm the success of the switch, and conducts continuous monitoring to check the integrity of the trust chain under the new KSK single-signature strategy.

DNS Technical Coordinator (HSM Administrator): After receiving confirmation of the successful global deployment by the Main RSP, submits a formal application for the revocation of the old KSK to the Principal of Network Operations Center, and notifies the Main RSP of the planned revocation time in advance; synchronizes the revocation status of the old KSK with the Main RSP, and urges the Main RSP to submit a request to delete the DS record corresponding to the old KSK to the IANA.

Principal of Network Operations Center (Management Decision-Maker): Approves the application for the revocation of the old KSK.

Internal Audit Administrator: Monitors the process of revoking the old KSK key to ensure compliance.

6) Completion of Rollover Closure and Archiving of Process Documents

The tasks executed during this phase are as follows:

DNS Operations Engineer (HSM Operator): Marks the old KSK as ""revoked"" and performs offline isolation storage after confirming the completion of DS deletion and the passage of an additional TTL security waiting period; applies for the release of a formal KSK rollover completion notice; collects all process documents of the rollover (plan, key verification documents, transmission logs, collaboration records, monitoring logs, etc.) and organizes them into a complete archive.

DNS Technical Coordinator (HSM Administrator): Sends a formal rollover completion notice to the Main RSP to confirm the formal conclusion of the rollover collaboration between both parties.

Principal of Network Operations Center (Management Decision-Maker): Approves the application for the release of the formal KSK rollover completion notice, confirming the successful completion of the annual KSK rollover for the corresponding gTLD.

Internal Audit Administrator: Conducts a full-process compliance review and summary.

3. Emergency KSK Rollover Process

1) Event Confirmation and Emergency Notification
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Initiates an emergency KSK rollover application in a timely manner for emergency rollovers triggered by serious security incidents such as KSK leakage, loss, or tampering.

DNS Technical Coordinator (HSM Administrator): Notifies the Main RSP via a dual channel of phone and encrypted email (including the type of incident, severity, and emergency rollover activation information), establishes a 24/7 emergency collaboration group, and confirms the emergency communication mechanism; completes the emergency event and rollover activation notification.

Principal of Network Operations Center (Management Decision-Maker): Reviews the emergency KSK rollover application, confirms the initiation of the emergency rollover, issues an emergency rollover activation order, and grants corresponding authorization.

2) Emergency Generation of New KSK and Corresponding DS Records
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Generates an emergency new KSK key pair and the corresponding DS record, and completes the format and consistency verification.

DNS Technical Coordinator (HSM Administrator): Verify the consistency between the public key and the DS record; synchronizes the progress of the emergency KSK key generation with the Main RSP, and confirms the encrypted transmission method for the new KSK public key and DS record in emergency situations.

Internal Audit Administrator: Monitors the entire key generation process to ensure compliance and prevent secondary leakage.

3) Emergency Activation of the New KSK and Submission to the Main RSP
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Disables the old KSK in the DNSSEC system, directly enables the new KSK for signing, verifies the signature logs to confirm the effectiveness, and conducts 24/7 real-time monitoring.

DNS Technical Coordinator (HSM Administrator): Submits the file to the Main RSP via the

emergency encrypted channel, sends an emergency submission notice, urges the Main RSP to carry out emergency deployment and resolution loading, and synchronizes the file receipt and deployment progress in real time.

Internal Audit Administrator: Monitors the compliance of the transmission process of the new KSK and DS record files.

4) Cooperation with the Main RSP to Complete the Emergency Deployment of the New DS Record in the IANA Root Zone System and Restore the DNSSEC Trust Chain
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Continuously monitors the operational status of the new KSK signing system 24/7, promptly resolves faults to ensure the continuity of the signing service; verifies the global resolution effectiveness of the new KSK/DS record and the integrity of the DNSSEC trust chain through global emergency test nodes.

DNS Technical Coordinator (HSM Administrator): Conducts real-time collaboration with the Main RSP 24/7, tracks the emergency deployment progress of the Main RSP in the IANA root zone system; obtains confirmation of the successful deployment by the Main RSP and the restoration of the trust chain; reports the work progress to the Principal of Network Operations Center every 4 hours.

Principal of Network Operations Center (Management Decision-Maker): Reviews the progress of the emergency rollover work and confirms the initial restoration of the DNSSEC service.

5) Emergency Rollover Closure and Incident Review
The tasks executed during this phase are as follows:
DNS Operations Engineer (HSM Operator): Updates the key inventory, confirms the normal operation of the new KSK; cooperates in the closure work, archives emergency collaboration records, and conducts post-incident review, analysis, and summary.

DNS Technical Coordinator (HSM Administrator): Sends an emergency rollover completion notice to the Main RSP to synchronize core information; provides the Main RSP with the non-sensitive root cause analysis results of the incident and the security improvement measures of our side; confirms the formal conclusion of the emergency rollover collaboration.

Principal of Network Operations Center (Management Decision-Maker): Reviews the emergency rollover archive and improvement report, issues an emergency KSK rollover completion notice, and orders the relevant teams to implement the security improvement measures in the report to prevent similar incidents from happening again.

Internal Audit Administrator: Monitors the full-process post-incident security review, analyzes the root cause of the incident, and implements security rectification measures; issues an emergency incident root cause analysis and security improvement report.