DNSSEC 4.14 KSK Rollovers

Service Model and DNSSEC RSP Role

Unstoppable Domains will rely on a MAIN RSP for MAIN RSP capabilities. As the DNSSEC RSP, our primary role is to assist in coordination of DS record changes between the MAIN RSP and IANA through the Root Zone Management (RZM) interface.

Unstoppable Domains intends to apply for MAIN RSP approval and may transition to using our own MAIN RSP infrastructure once approved. However, the coordination procedures and IANA communication protocols described in this response remain consistent regardless of whether the MAIN RSP is an external provider or our own approved infrastructure.

Non-Emergency (Planned) Rollover Process

Non-emergency KSK rollovers are expected to be a scheduled maintenance activities conducted according to the MAIN RSP's maintenance calendar, typically annually for KSK rotations. These follow standard processing timelines and may include advance notification to MAIN RSP stakeholders (e.g. registrars, recursive DNS operators, monitoring services, etc). The planned rollover process consists of five key phases:

Phase 1: Key Pre-publication We, the DNSSEC RSP pre-publishes the new DNSKEY RRSet in the zone according to the agreed maintenance timeline and coordinates with MAIN RSP to prepare the corresponding DS record for IANA submission. MAIN RSP is expected to validate the DS record to ensure accuracy before submission.

Phase 2: DS Record Submission MAIN RSP is expected to submit the new DS record to IANA through the RZM interface during standard business hours, ensuring both old and new DS records will exist simultaneously during the rollover period to maintain the chain of trust.

Phase 3: Standard Processing The MAIN RSP DS record change is expected to follow IANA's standard processing timeline through the RZM interface with the typical 2.5-day processing window for DS record publication in the root zone.

Phase 4: Key Activation Once the new DS record appears in the root zone, the MAIN RSP is expected to coordinate with us, the DNSSEC RSP, to mark the new key as ready. The key can be promoted to active status for signing operations and automatic timing can be initiated for the old key phase-out period.

Phase 5: Old Key Removal After TTL expiration periods have passed according to published timelines, MAIN RSP is expected to coordinate removal of the old DS record from IANA through the RZM interface and validate that only the new DS record remains active in the root zone.

Emergency Rollover Process

Emergency KSK rollovers are unscheduled events triggered by security incidents such as key compromise, cryptographic vulnerabilities, operational errors, or other urgent circumstances that threaten the integrity of the DNSSEC chain of trust. These follow the same five-phase technical process but with critical differences in timing, communication, and coordination protocols:

Phase 1: Key Pre-publication We, the DNSSEC RSP immediately pre-publishes the new DNSKEY RRSet in the zone using emergency key generation procedures and coordinates with MAIN RSP to prepare the corresponding DS record for urgent IANA submission. MAIN RSP is expected to perform expedited validation of DS record integrity.

Phase 2: DS Record Submission The MAIN RSP is expected to immediately submit the new DS record to IANA through the RZM interface, ensuring both old and new DS records will exist simultaneously during the emergency rollover period to maintain the chain of trust.

Phase 3: Expedited Processing The MAIN RSP is expected to submit the DS record change request through the RZM interface and immediately contact IANA's emergency call center to expedite processing, reducing response time to near-instant activation based on the severity classification and IANA's emergency procedures.

Phase 4: Key Activation Once the new DS record appears in the root zone, the MAIN RSP is expected to immediately coordinate with the DNSSEC RSP to mark the key as ready. The key is immediately promoted to active status for signing operations and automatic timing is initiated for the old key phase-out period.

Phase 5: Old Key Removal After minimum TTL expiration periods have passed, the MAIN RSP is expected to coordinate expedited removal of the old DS record from IANA through the RZM interface and validate that only the new DS record remains active in the root zone.

Coordination with External MAIN RSP

Non-Emergency Coordination: For planned rollovers, MAIN RSP is expected to maintain scheduled communication with us, the DNSSEC RSP, according to the MAIN RSP’s published maintenance calendar. We, the DNSSEC RSP, provide advance notification (typically one quarter ahead) of planned key ceremonies, generate new KSK material following standard ceremony procedures, and provide the MAIN RSP with DS record data during normal business hours with standard validation timeframes.

Emergency Coordination: For emergency situations, the MAIN RSP is expected to maintain 24/7 communication channels with us, the DNSSEC RSP, including dedicated emergency contact procedures for urgent rollover situations. We, the DNSSEC RSP, implement immediate key generation procedures (which may use virtual meetings), provide DS record data on an expedited basis, and coordinate continuous communication throughout the emergency response timeline.

DS Record Coordination: We, the DNSSEC RSP, generate new KSK material following key ceremony procedures and provide the MAIN RSP with the corresponding DS record data including key tag, algorithm identifier, digest type, and key digest. The MAIN RSP is expected to validate this information against the published DNSKEY records before submission to IANA.

Timing Coordination: The MAIN RSP is expected to coordinate precise timing with us, the DNSSEC RSP, to ensure proper sequencing: DS record publication in the root zone must occur before we, the DNSSEC RSP, begin using the new KSK for signing operations. This prevents validation failures during the rollover transition.

Validation Procedures: The MAIN RSP is expected to verify DNSKEY record publication by us, the DNSSEC RSP, and confirm DS record accuracy before and after IANA submissions. The MAIN RSP is expected to also coordinate post-rollover validation to ensure proper chain of trust establishment.

IANA Communication and Coordination

Standard Operations: The MAIN RSP is expected to submit all routine DS record changes through IANA's RZM interface, where the MAIN RSP is expected to manage change requests and track processing status.

Emergency Procedures: For emergency rollovers, we expect the MAIN RSP to follow a two-step process: first submitting the change request through the RZM interface to establish the formal record, then immediately contacting IANA's emergency call center to expedite processing. This ensures proper documentation while enabling rapid response to security incidents.

Coordination Timing: The MAIN RSP is expected to monitor the RZM interface to confirm DS record publication and coordinate activation timing with us, the DNSSEC RSP. For emergency situations, the MAIN RSP is expected to maintain continuous communication with both IANA and us, the DNSSEC RSP, throughout the rollover process to ensure synchronized operations.

Documentation and Transparency: The MAIN RSP is expected to document and publish to their, the MAIN RSP, website maintenance event history page all emergency rollover activities, following the transparency model established by IANA's Key Signing Ceremonies. The MAIN RSP is expected to provide detailed post-incident reports including timeline, coordination activities, and lessons learned.

Independent of MAIN RSP documentation activities, we, the DNSSEC RSP, publish the results of all KSK and ZSK maintenance events — both planned and emergency — to the Unstoppable Domains DNSSEC RSP website maintenance event history page, following the transparency model established by IANA's Key Signing Ceremonies. For emergency rotations, this includes timeline documentation, actions taken, and post-incident analysis.

Technical Implementation Details

The DS records consist of four critical components: key tag (identifier), algorithm (cryptographic algorithm used), digest type (hash algorithm), and key digest (hash of the DNSKEY). These values establish the cryptographic link between the child zone KSK and the parent zone (root) for chain of trust validation.

DS record validation involves verifying the correspondence between DNSKEY records published by us, the DNSSEC RSP, and the DS records the MAIN RSP is expected to submit to IANA. The MAIN RSP is expected to use industry-standard tools such as ldns-key2ds to generate and validate DS records from published DNSKEY records provided by us, the DNSSEC RSP.

The MAIN RSP is expected to maintain a validation process that includes cross-referencing the DS record components against the published DNSKEY to ensure mathematical accuracy, verifying algorithm compatibility with IANA's supported cryptographic standards, and confirming proper formatting for RZM interface submission. This technical validation ensures the integrity of the DNSSEC chain of trust before any coordination with IANA.