Proposal for Root Zone KSK Algorithm Rollover

This proposal describes the technical considerations for a future algorithm rollover to the Key Signing Key of the DNS root zone (Root KSK). The Root KSK serves as the global trust anchor for DNSSEC and is managed as part of the IANA functions. We seek feedback from the community to help refine and finalize our approach before implementing operational and procedural updates.

Executive Summary

This proposal describes a plan for a future DNSSEC algorithm rollover of the DNS root zone, transitioning the algorithm from RSA with SHA256 (numerically algorithm 8 in the DNSSEC standard) to ECDSA P-256 with SHA256 (algorithm 13). The Root Zone KSK is a critical trust anchor, and this transition aims to enhance cryptographic strength while managing operational risks such as response size and resolver compatibility.

The plan presented here follows a common double-signing approach for DNSSEC transitions, avoiding the need for pre-publication of the new algorithm's key to comply with mandatory algorithm rules in RFC 6781. Prior to the algorithm transition, the size of the RSA-based Zone Signing Key (ZSK) will be reduced from 2048 to 1536 bits to reduce the possible need for truncation and retransmission over TCP.

This proposal defines milestones that span a four-year period, from generation of a new ECDSA key in 2027 to serve as the new Root KSK, to final decommissioning of the replaced Root KSK in 2030. The algorithm rollover is structured around quarterly key signing ceremonies.

This proposal incorporates findings from the *Root Zone DNSSEC Algorithm Rollover Study* and addresses all recommendations.

Community feedback on the current proposal is invited to help refine the proposed implementation prior to operational execution.

Background

Cryptographically signing the root zone with DNSSEC began in 2010 using RSA-based algorithms. Although the KSK was first replaced in 2018 (an event known as a rollover), it continues to rely on the same RSA cryptographic algorithm. The next rollover, already in progress, and scheduled to transition on 11 October 2026, will continue to use the same

algorithm. There are no established mechanisms for transitioning the root zone to a different signing algorithm.

The Second Security, Stability, and Resiliency (SSR2) Review, published in 2021, highlighted this gap and recommended that ICANN develop a clear and predictable plan to allow for changes to the cryptographic algorithm used in the root zone. To support this work, ICANN conducted the *Root Zone Algorithm Rollover Study* in 2024 (the "Study") which assessed resolver and authoritative server support for alternative algorithms, analyzed potential rollover methodologies, and evaluated operational risks.

Algorithm Selection

The next algorithm for the Root KSK shall be ECDSA using the P-256 curve. The adoption of this algorithm for DNSSEC signing in the root zone is consistent with the guidance provided in the Study. The Study recommended that any successor to RSA/SHA-256 must already be standardized through the IETF and designated as a required implementation for DNSSEC validation. ECDSA P-256 with SHA256 meets this requirement, being specified in RFC 9904, published in late 2025, as a mandatory algorithm for both signing and validation.

The study recommended that a candidate algorithm demonstrate sufficient operational deployment in the DNS ecosystem prior to introduction at the root. ECDSA P-256 has already been adopted by numerous top-level domains. Its implementation is widely supported across major open-source and commercial DNS software, including BIND, Unbound, Knot Resolver, and PowerDNS, as well as by major resolver operators. This broad adoption indicates that the validating resolver base is already capable of processing ECDSA signatures.

Operational considerations also include the ability to manage keys within current hardware and procedural environments. The study stressed the importance of diversity in hardware security module (HSM) support and cryptographic implementations, while also acknowledging the diminishing availability of devices certified under older standards. After the publication of the study, the KSK Operator and ZSK Operator DNSSEC Practice Statements (DPS) were updated to allow for devices that meet FIPS 140-3 Level 3 or greater, providing additional vendor support. IANA has deployed Thales Luna G7 HSMs into its operational environment to hold the upcoming KSK-2024, which support ECDSA key generation and signing within the operational parameters of the DPS.

Prerequisite: Reducing the RSA ZSK Size

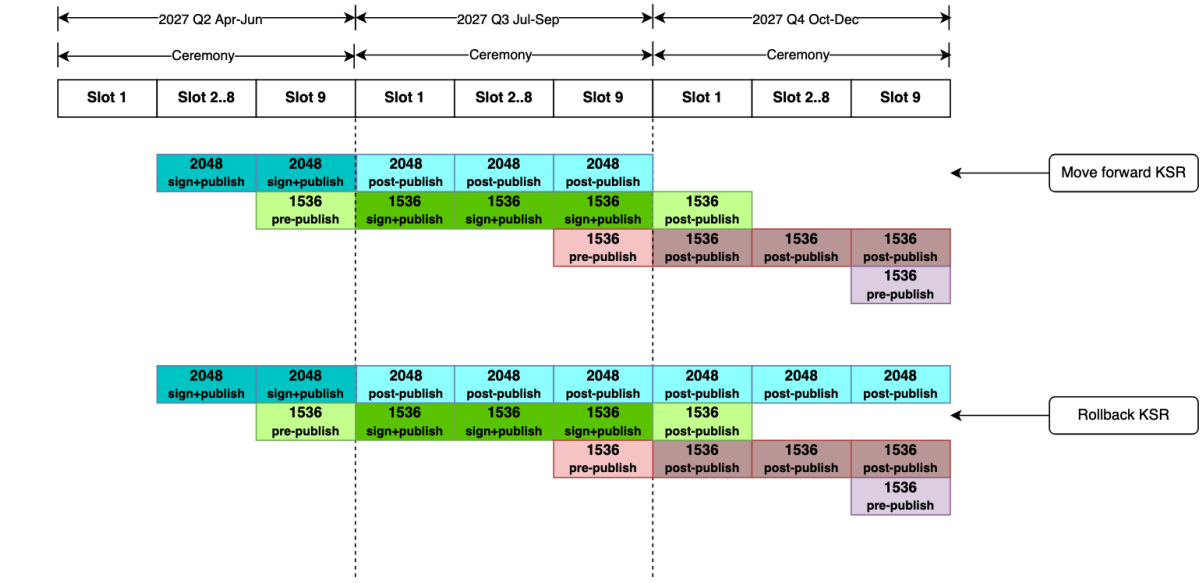
Given the choice to utilize the double-signing approach and the desire to keep DNS response sizes from exceeding certain thresholds that would trigger fragmentation, it is necessary to reduce the size of the RSA ZSK during the algorithm transition.

The root zone's RSA ZSK size has been 2048 bits since October 2016. This configuration has not demonstrated problems during the first (2018) and second (2025) KSK rollovers because during these non-algorithm rollovers only the size of the DNSKEY response is affected. DNSKEY queries to the root zone comprise less than half of one percent of the total queries seen by the root servers.

If a resolver receives a truncated message in response to a DNSKEY query, it can retry over TCP and any impact to the root server system is negligible.

During a double-signature algorithm rollover, however, the root zone referral and NXDOMAIN responses will also increase in size. This, combined with the 2020 DNS Flag Day effort to promote the use of 1232 bytes as a default maximum UDP buffer size, means that with double-signing and a ZSK of 2048 bits, most root server responses would lead to truncation and retries over TCP.

To reduce the prevalence of this situation, the root zone's RSA ZSK will be decreased in size to 1536 bits as an early step in the algorithm rollover process. The RSA key size of 1536 bits was chosen as the point halfway between 1024 and 2048 and because it permits almost all responses (with the exception of DNSKEY responses during quarterly ZSK rollovers) to remain under 1232 bytes during the algorithm rollover.



The transition to a 1536-bit RSA ZSK will begin in the same calendar quarter as the algorithm rollover. The 1536-bit RSA ZSK will be pre-published in the last slot of the second quarter. Starting in the first slot of the third quarter, the root zone will be signed with the 1536-bit RSA ZSK. During this entire second quarter, the previous 2048-bit RSA ZSK will be post-published in

case it becomes necessary to revert to the previous configuration. This means that the typical quarterly rollover for the 2048-bit RSA ZSK will not occur in that quarter.

This schedule provides the Root Zone Maintainer approximately 120 days to remediate any problems that might arise during the transition. The RSA key size for ZSKs will stay at 1536 bits until the end of the algorithm rollover, which will take approximately 3 years.

Operational Plan

The algorithm rollover process follows the same general structure as previous KSK rollovers but uses a distinct set of phase identifiers (AA through HH) to differentiate it from non-algorithm rollovers. Phases are aligned to calendar quarters (i.e. beginning January 1, April 1, July 1, and October 1), but a phase may span multiple quarters if the process is extended or backed out. Each quarter is divided into nine publication slots of approximately ten days, with the final slot extended as needed to complete the quarter.

Historically, KSK and ZSK changes have been introduced in different slots. For this algorithm rollover, KSK and ZSK operations will occur in the same slots to align with rules relating to algorithm choice in the DNSSEC standard; in these cases publication will be aligned to the KSK slots (Slots 2–8).

Key Signing Ceremonies

Key signing ceremonies produce the signed key response (SKR) used to publish DNSKEY RRsets and signatures for the following quarter. Ceremonies occur once per quarter and normally sign a single KSR. However, during a rollover, ceremonies may sign multiple KSRs to prepare SKRs for each possible state in the upcoming quarter:

- Forward transition (e.g., CC→DD)
- Extension (e.g., DD→DD)
- Backout (e.g., DD→CC)
- Prolonged backout (e.g., CC→CC)

Only one SKR set becomes active, depending on whether the next quarter begins with a forward move, extension, or backout. The root zone will reflect that decision beginning with the Slot 2 publication of the quarter.

The prolonged backout is necessary because a backout scenario could be enacted after a ceremony generated the SKRs for that quarter.

Backout and extension scenarios

Backing out of the rollover process is a significant step. There is no contingency planned after a backout, other than to keep the stable backout state indefinitely. If there is a backout situation, the causes that led to a backout will be studied and the results will be used as input for a new KSK rollover process. In short, once a backout is performed, the process is essentially set to the end of the previous phase. The only exception is once a KSK is revoked, the backout action is to go to the next phase instead of going back, since a revoked key must not reappear unrevoked in the keyset data.

Extending the current phase means that the next phase of the KSK rollover process is postponed by at least one calendar quarter.

Phases

Phase AA: Key Generation

Description
Generate the new ECDSA KSK and establish secure storage across both Key Management Facilities (KMFs).

Root zone changes
None.

Key ceremony actions
- At the first KMF, generate the ECDSA KSK in one HSM and restore the new key to a second HSM in that same facility.
- Prepare encrypted backups and transfer packages for these new keys aligned to DPS controls.
- At the second KMF, store the key backups in an administrative ceremony as soon as possible.

Phase BB: Key Replication

Description
Replicate the ECDSA KSK across all production HSMs in the second KMF to achieve operational readiness.

Root zone changes
None.

Key ceremony actions
- At the second KMF, restore the ECDSA KSK into all production HSMs.

Phase CC: Initial Signature Generation (ECDSA)

Description
Begin generating SKRs that contain ECDSA signatures to be published later.

Root zone changes
None. SKRs generated in this phase are published in the next quarter marking the start of the next phase.

Key ceremony actions
- Generate the following SKRs:
  - CC → DD: Primary transition to the next phase where signatures will be introduced
  - DD → CC: Backout transition to remove the ECDSA signatures
  - CC → CC: This is an alternate to the primary transition to extend the current phase, delaying the transition to the next phase at least one quarter.

Phase DD: Signature Publication (ECDSA)

Description
Publish signatures generated using the ECDSA KSK and ZSK without publishing their corresponding DNSKEY records.

Root zone changes
- ECDSA signatures first appear in the root zone on the 11th day of the quarter (Slot 2) covering all signable records. Signatures are generated from unpublished ECDSA KSK and ZSKs.

Timing and backout
- Backout using DD → CC (removing the ECDSA signatures) at any time during the quarter.

Key ceremony actions
- Generate the following SKRs:
  - DD → EE: Primary transition to the next phase that will introduce the ECDSA DNSKEYs
  - EE → DD: Backout transition to delay or remove the ECDSA keys
  - DD → DD: This is an alternate to the primary transition to extend the current phase, delaying the transition to the next phase at least one quarter.
  - CC → CC: Prolonged backout which is necessary should the DD → CC backout occur following the date of this ceremony.

Phase EE: Key publication and double signing (RSA and ECDSA)

Description
Publish the ECDSA DNSKEYs and sign the root zone using both RSA and ECDSA keys.

Root zone changes

- ECDSA KSK and ZSK DNSKEYs first appear at Slot 2 (11th day) of the quarter.
- The root zone is dual-signed for the duration of this phase.

Timing and backout

- Backout using EE → DD (removing the ECDSA DNSKEYs) at any time during the quarter.

Key ceremony actions

- Generate the following SKRs:
  - EE → FF: Primary forward transition that will begin the revocation of the RSA KSK. This SKR will be used after almost two years in phase EE after resolvers have updated trust anchors.
  - EE → EE: This is an alternate to the primary forward transition to extend the current phase. This SKR will be used for almost two years while resolvers update their trust anchors.
  - DD → DD: Prolonged backout which is necessary should the EE → DD backout occur following the date of this ceremony.
  - FF → GG: Fast forward the revocation by removing the RSA keys and signatures from the root zone. This set is not used during Phase EE, but is instead prepared for Phase FF.

Phase FF: Revocation of RSA KSK

Description

Revoke the RSA KSK and remove all RSA keys and signatures from the root zone.

Root zone changes

- Beginning on the 11th day of the quarter (Slot 2), the RSA KSK will appear with the REVOKE bit set. The RSA ZSK will remain published as will its signatures.
- Beginning on the 81st day of the quarter (Slot 9), the RSA KSK and ZSK and their signatures will be removed from the root zone.

Timing and backout

- As with other rollovers, after a KSK is revoked, the process does not back out to an unrevoked state; the next state is removal of the RSA key and its deletion.
- There are SKRs to fast-forward the removal of the revoked key and signatures that were prepared in Phase EE for this phase.

Phase GG: First Deletion

Description

Destroy the RSA KSK material present the first KMF.

Root zone changes
None.

Key ceremony actions
- At the first KMF, destroy RSA KSK material from all HSMs.

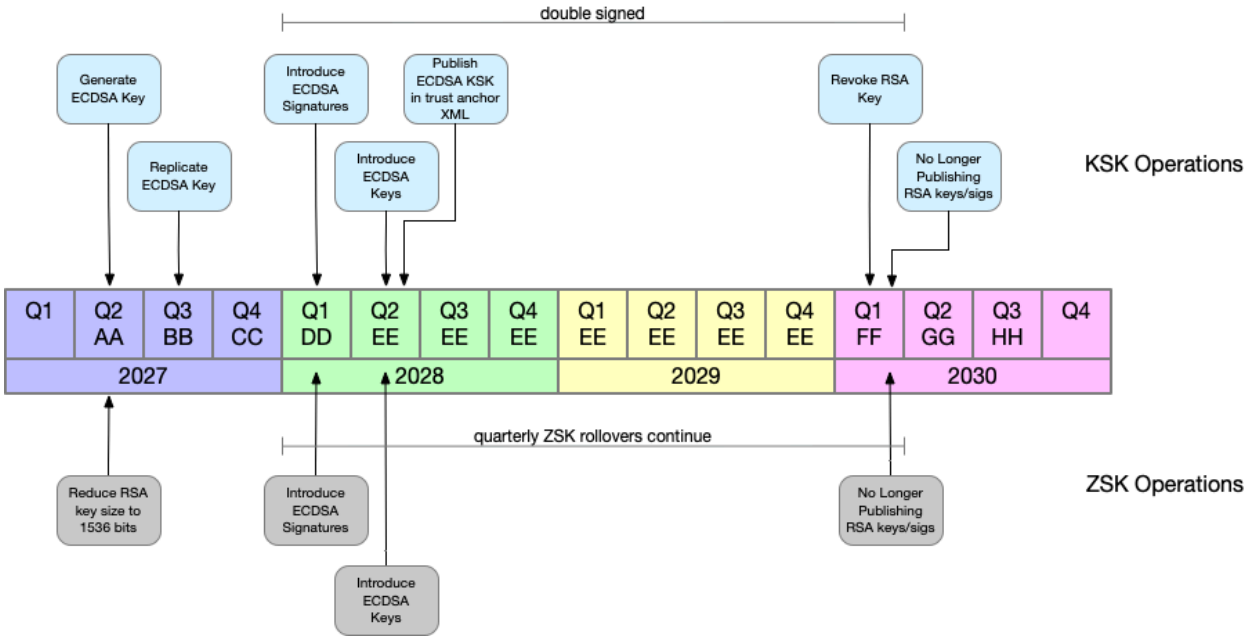
Phase HH: Second Deletion

Description
Complete the destruction of RSA key material.

Root zone changes
None.

Key ceremony actions
- At the second KMF, destroy RSA KSK material from all HSMs.

Timeline



Trust Anchor Distribution

IANA publishes information on the DNSSEC trust anchors through the mechanisms described in [DNSSEC Trust Anchor Publication for the Root Zone](#) (RFC 9718), specifically through

publication of the root-anchors.xml file. This file is used by resolvers and operators to maintain and update their trust anchors.

The new ECDSA key will be added to the root-anchors.xml file after the RFC 5011 30-day hold-down timer has elapsed after the key is introduced to the root zone. At that point, the ECDSA key will have begun to be accepted automatically by compliant resolvers, and there is no reason to delay its inclusion in the published trust anchor set. Earlier publication could conflict with the mandatory algorithm rules in RFC 6840, Section 5.11, which states that a signed zone MUST include a DNSKEY for each algorithm present in the zone's DS RRset and *expected trust anchors for the zone*. Information on the KSK will be published on the IANA website following generation, and provide a means to cross-reference the new key once it appears in the DNS root zone.

After the RSA key is revoked, the root-anchors.xml file will be updated, with the notAfter attribute set to the date when the RSA-based KSK DNSKEY record was published with the revocation bit set. Because RFC 9718 provides no normative guidance on refresh frequency, this update will occur only after the revoked key has appeared in the DNS, to avoid a situation in which delayed revocation could create inconsistencies with the root-anchors.xml file.

Risk Mitigation

The proposed algorithm rollover introduces inherent operational and technical risks. This section outlines the identified risks, backout options, and contingency measures integrated into the implementation plan.

- **Backout SKRs:** Each milestone includes additional Signed Key Responses (SKRs) generated for backout use. These SKRs allow us to revert to a previous signing state in the event of unexpected issues.
- **Flexible Phase Scheduling**: Each rollover phase has built-in flexibility and can be extended across multiple quarters. This provides time to address deployment challenges, collect telemetry data, and respond to feedback from stakeholders.
- **Communications and Outreach:** Communications will provide early and ongoing notifications to resolver operators, and other stakeholders. This outreach will include mailing lists, ICANN announcements, relevant meetings, and technical conferences to ensure wide awareness of key rollover events and trust anchor changes.

References and Terminology

References:

- Operational Plans for the Root KSK Rollover (2018)
- Proposal for Future Root Zone KSK Rollovers (2019)

- Root Zone Algorithm Rollover Study (2024)
- DNSSEC Practice Statement for the Root Zone KSK Operator (2025)

Term	Definition
DPS	The DNSSEC Practice Statement (DPS) describes the policies and operational practices used to manage cryptographic keys and signatures within a DNSSEC-secured zone. It defines how keys are generated, stored, used, rolled over, and retired, and outlines security controls to ensure the integrity and authenticity of the zone's signing process.
KMF	A key management facility (KMF) is a secured environment used to perform and control cryptographic key operations such as generation, activation, backup, storage, and destruction. In DNSSEC operations, the KMF encompasses the systems, hardware security modules (HSMs), and administrative procedures that protect key material throughout its lifecycle.
KSK	A key signing key (KSK) is a cryptographic key pair used in DNSSEC to sign the DNSKEY resource record set (RRset) of a zone. In the context of the DNS root zone, the KSK serves as the trust anchor for DNSSEC validation and is configured as such by validating resolvers to establish the chain of trust.
KSK-2024	KSK-2024 is a codename used in operations to refer to the KSK that was generated in 2024, and that currently is the presumptive operative trust anchor to be in place by the end of 2026.
KSR	A key signing request (KSR) is a file that contains the public keys of the ZSKs for the root zone that are to be signed in a ceremony operated by IANA.
SKR	A signed key response (SKR) is a list of DNSSEC signatures on the keys given in a KSR.
Slot	As described in the DPS, a *slot* is a fixed unit of operational time. For the root zone, slots are typically ten days, which means that nine slots make up each calendar quarter. DNSSEC activities for the root zone, such as key management and signing operations, are scheduled and referenced by their designated slot number within the quarter.
ZSK	A zone signing key (ZSK) is a cryptographic key pair used in DNSSEC to sign the resource record sets (RRsets) within a zone, excluding the DNSKEY RRset itself. The ZSK's private key generates the digital signatures (RRSIG records) that protect the integrity and authenticity of the zone data.