Public Comment Summary Report

Proposed Root KSK Algorithm Rollover

Open for Submissions Date:
Tuesday, 03 February 2026

Closed for Submissions Date:
Monday, 06 April 2026

Summary Report Due Date:
Monday, 04 May 2026 (Extended from Monday, 27 April 2026)

Category: Technical

Requester: ICANN org

ICANN organization contact(s):
james.mitchell@iana.org

Open Proceeding Link:
https://www.icann.org/en/public-comment/proceeding/proposed-root-ksk-algorithm-rollover-03-02-2026

Outcome:
ICANN org received 12 submissions on the Proposed Root Zone KSK Algorithm Rollover, including a late submission from the ICANN Security and Stability Advisory Committee (SSAC). Responses ranged from broad support for the proposal to technical concerns, principally regarding the reduction of the RSA Zone Signing Key from 2048 to 1536 bits and the absence of defined criteria for triggering phase scheduling adjustments. No structural changes to the rollover plan were made as a result of the proceeding. ICANN org will proceed with the algorithm rollover as proposed and will publish phase transition criteria and conduct targeted outreach to the operator community ahead of the transition.

Public Comment provided a useful record of community views on a technically complex operational proposal. The input confirmed broad support for the proposal's overall direction and identified specific areas where additional documentation will strengthen the operational basis for the rollover. This summary report serves as the primary record of ICANN org's responses to the concerns raised during the proceeding.

Section 1: What We Received Input On

The DNS root zone has been signed using RSA/SHA-256 (Algorithm 8) since DNSSEC was first deployed for the root in 2010. While RSA/SHA-256 remains cryptographically secure, the DNSSEC ecosystem has matured significantly since then: ECDSA P-256 (Algorithm 13) is now the recommended algorithm for DNSSEC signing under RFC 8624 and its successor RFC 9904, has surpassed RSA globally in deployment across signed zones, and is supported as a mandatory implementation algorithm by all major DNSSEC resolver software. Transitioning the

root zone KSK to ECDSA P-256 aligns the DNS root with current best practice, reduces DNS response sizes, and is consistent with Recommendation 23.2 of the second Security, Stability and Resiliency Review (SSR2), which called on ICANN org to evaluate and plan for an algorithm rollover.

The Public Comment proceeding sought input on the proposed approach for executing this transition. The proposal outlined a phased double-signing rollover in which both the existing RSA KSK and a new ECDSA KSK would be simultaneously present in the root zone for approximately two years, allowing validating resolvers to update trust anchors before the RSA KSK is revoked and removed. A prerequisite reduction of the RSA Zone Signing Key (ZSK) from 2048 to 1536 bits was also proposed, to keep dual-signed DNS responses within the 1232-bytes reducing truncation and fallback to TCP. The proposal included associated updates to key management documentation, ceremony procedures, and a mechanism for adjusting the rollover schedule at quarter boundaries in response to operational conditions. The proceeding invited feedback on the technical approach, risk management, implementation plan, and overall readiness for executing the algorithm rollover.

Section 2: Submissions

Organizations and Groups:

Name	Submitted by	Initials
Root Server System Advisory Committee	RSSAC Staff	RSSAC
Verisign, Inc.	Duane Wessels	DW
Registries Stakeholder Group		RySG

Individuals:

Name	Affiliation (if provided)	Initials
Gbemisola Esho	AFRALO	GE
Joshua Ibitoye	SouthEast Missouri State University	JI
Nhat Huy Nguyen		NHN
NITIN WALIA	DATA.IN	NW
Benson King'Ori Mugure		BM
Diksha Neeladoo B. Simmandree		DS
Jieling Xie		JX
Michael St Johns		MS

Section 2a: Late Submissions

ICANN org accepted the following submission received after the close of the Public Comment period. This submission has been considered alongside the timely submissions in the analysis in Section 3.

Name	Submitted by	Initials
Security and Stability Advisory Committee (comments)	ICANN SSAC Staff	SSAC

Section 3: Summary of Submissions

ICANN appreciates the time, dedication, and participation of all who contributed to this proceeding. There were 12 submissions to the Public Comment proceeding on the Proposal for Root Zone KSK Algorithm Rollover, including one late submission from the SSAC.

Of the 12 submissions, three organizations (RSSAC, RySG, and Verisign [DW]) expressed support for the proposal. Four individual submitters expressed support while raising specific operational or technical recommendations [JI, NHN, NW, GE]. Four submitters raised concerns or objections to elements of the proposal [MS, BM, DS, JX]. The SSAC expressed support for the proposal's overarching goal while providing specific technical recommendations on the ZSK size reduction and implementation timeline.

3.1 RSA Zone Signing Key (ZSK) Size Reduction

Comment Summary:

The proposed reduction of the RSA ZSK from 2048 to 1536 bits was the most widely commented issue in the proceedings. Several submitters [MS, BM, DS, JX] raised concerns that 1536 bits is not a standard RSA key size recognized by NIST, that the reduction lowers the ZSK's effective security level from approximately 112 bits to approximately 90–96 bits, and that this degraded posture would persist for the approximately three-year duration of the rollover. Others [JI, NW, NHN] acknowledged the trade-off as reasonable in principle but called for more explicit justification and monitoring commitments. RSSAC and RySG expressed no substantive concerns with the reduction. Verisign [DW] submitted an accompanying empirical analysis of root server response size data supporting the 1536-bit choice, finding that the combination of a 1536-bit RSA ZSK and an ECDSA ZSK would push approximately 1–5% of responses above the 1232-byte limit. SSAC assessed the reduction as operationally advisable given the approximately 110-day per-key exposure window, and recommended that the final plan include an independent estimate of the computational cost of attacking a 1536-bit key within that window.

ICANN org Analysis:

The 1536-bit size was selected to provide maximum cryptographic strength within the constraint of keeping almost all root server responses under 1232 bytes (DNSKEY responses during quarterly ZSK rollovers are an exception). Retaining a 2048-bit RSA ZSK during double-signing would cause a significant number of referral and NXDOMAIN responses to exceed that size, requiring widespread TCP fallback for the duration of the rollover. Verisign's empirical analysis, based on RSSAC-002 traffic data, confirms that the 1536-bit choice yields a substantially better response-size outcome than the 2048-bit alternative, with an estimated 1–5% of responses affected.

ICANN org concurs with the SSAC's analysis that each ZSK key's approximately 110-day exposure window, during which a key is actively used and publicly observable, is too short for a brute-force attack against a 1536-bit key to be feasible under current capabilities. The security reduction relative to a 2048-bit key is real but bounded by this operational window, and ICANN org considers this characterization a sufficient and appropriate basis for the decision.

ICANN org notes that while NIST key management guidance enumerates 1024, 2048, and 3072 bits as reference RSA key sizes, non-standard RSA key sizes are not unprecedented in DNSSEC operations: the root zone ZSK itself was previously 1280 bits, and other non-standard sizes are in operational use across the DNS ecosystem. The selection of 1536 bits reflects a deliberate engineering judgment to maximize cryptographic strength within the response-size constraint, and its security implications are addressed directly here.

3.2 Phase DD — ECDSA Signatures Published Without DNSKEYs

Comment Summary:
Several submitters questioned or objected to Phase DD, in which ECDSA signatures are published in the root zone before the corresponding ECDSA DNSKEY records appear. [BM] and [NW] argued that the phase should be eliminated, contending that publishing signatures without DNSKEYs provides no security benefit and that ECDSA public keys are in any case recoverable from the signatures themselves. [MS] stated that that no justification was provided for withholding the DNSKEYs, and additionally raised what he characterized as a phase logic anomaly, arguing that Phase DD should not include CC-CC signing activity.

ICANN org Analysis:
Phase DD serves two distinct purposes that are addressed in turn.

The first is operational. ICANN org acknowledges that a full quarter is not strictly technically necessary for the purposes of Phase DD alone. However, key signing ceremonies, SKR generation, and publication schedules are all structured around calendar quarters, and introducing sub-quarter phase transitions would require multiple DNS transitions within a single quarter, adding operational complexity and increasing the risk of error. The quarterly structure provides a clean, well-understood window for assessment and monitoring before proceeding to Phase EE, and is consistent with the approach taken in prior KSK rollovers. Critically, as SSAC notes, if resolvers failing to process ECDSA signatures correctly are identified during Phase DD, the plan allows the phase to be backed out or extended by one or more additional quarters while remediation is pursued before the DNSKEYs are introduced.

The second is cache coherency. If ECDSA signing of zone records began simultaneously with publication of the DNSKEYs, there would be a window during which a resolver could receive and cache the new ECDSA DNSKEY records while still holding previously-cached resource records that carry only RSA signatures, whose ECDSA signatures had not yet propagated into resolver caches. This could result in resolvers attempting to validate cached responses with a newly-acquired ECDSA key and finding no corresponding ECDSA RRSIG, which could lead to

validation failures if clients enforce mandatory algorithm signing rules in RFC 6840. Phase DD addresses this by ensuring ECDSA signatures are distributed throughout the validating resolvers ecosystem for a full quarter before DNSKEYs are published, so there is no inconsistency window at the start of Phase EE.

The argument that ECDSA public keys can be mathematically recovered from the signatures does not bear on either of these purposes. Phase DD is not intended to conceal the public keys, which are published during the key ceremony in which they were generated.

The purported logic anomaly with CC-CC activity in Phase DD is not an anomaly. CC→CC is a prolonged backout SKR, necessary in the event that a DD→CC backout decision is made after the key signing ceremony for that quarter has already occurred. In that scenario, the active SKR set for the following quarter must return to CC-state, and the CC→CC SKR prepared at the Phase DD ceremony is the mechanism by which that is accomplished.

3.3 ZSK Algorithm Rollover as an Alternative

Comment Summary:

Several submitters [MS, BM, JX, DS, NW] proposed transitioning the ZSK algorithm to ECDSA P-256 before undertaking the KSK algorithm rollover, arguing this would eliminate the need for the 1536-bit RSA ZSK reduction entirely. [MS] provided a detailed two-step rollover sequence; [BM] indicated Verisign's transition of .com and .net as evidence of feasibility, though Verisign's transition followed the same double-signing approach proposed here rather than a ZSK-first approach. SSAC addressed this alternative directly, noting that operating RSA and ECDSA ZSKs simultaneously without a corresponding RSA KSK would conflict with the mandatory algorithm signing rules in RFC 6840, and that draft-huque-dnsop-multi-alg-rules, which would relax those rules, has not been adopted by the IETF DNSOP working group.

ICANN org Analysis:

ICANN org appreciates the thoughtful engagement on this alternative, which reflects a genuine interest in preserving full ZSK cryptographic strength throughout the transition.

As SSAC notes, operating ECDSA and RSA ZSKs simultaneously without a corresponding RSA KSK would not comply with the mandatory algorithm signing rules established in RFC 6840. While it is reasonable to expect that well-known validating resolvers, whose implementations tend to be current and actively maintained, would handle such a configuration without issue, the root zone cannot be operated on that basis alone. The root zone is the global trust anchor for DNSSEC, and any operational decision that departs from established standards must account for the full range of resolvers and implementations in production use worldwide, including those that are older, less frequently updated, or operating in constrained environments. The potential for widespread and difficult-to-diagnose validation failures demands a conservative approach that remains within the bounds of protocol specifications.

Retaining the RSA ZSK at a reduced size during the transition is the more conservative of the two options. It complies fully with RFC 6840 and does not depend on either resolver implementation tolerance for non-conforming behavior or the future adoption of an IETF draft. This approach is comparable to the approach Verisign followed when transitioning .com and .net to ECDSA, which [BM] cited as a precedent but which in fact supports the proposed method rather than the ZSK-first alternative. As noted in section 3.1, the cryptographic strength of the 1536-bit ZSK during its approximately 110-day exposure window is currently considered adequate by SSAC and ICANN org. On balance, accepting a time-bounded and quantifiable reduction in ZSK key size is preferable to introducing a standards deviation of uncertain and variable impact across a globally heterogeneous resolver population.

3.4 Pre-Generated Signed Key Responses (SKRs)

Comment Summary:

[MS] and [NW] raised concerns about the security of pre-generated SKRs, noting that the access controls and custody boundaries governing pre-computed SKRs are not described in the proposal and that old transition-state SKRs could potentially be replayed after ICANN has moved to a subsequent phase. [BM] characterized pre-stored backout SKRs as a "cryptographic stockpiling" risk. [SSAC] supported the inclusion of backout SKRs and the plan's provisions for phase extension and schedule adjustment as appropriate operational safety valves.

ICANN org Analysis:

The generation of multiple parallel SKRs, covering forward, hold, and backout states, is existing operational practice and is not introduced by the algorithm rollover. The security controls, key management framework, and physical and logical protections governing SKR handling are established elements of ICANN org's root zone management operations. The concerns raised regarding replay and unauthorized use of backout SKRs are noted and taken under advisement.

3.5 Phase FF — RSA KSK Revocation Window

Comment Summary:

[MS] and [DS] argued that the proposed 70-day revocation publication window is insufficient, with [MS] contending that resolvers may hold a cached copy of the un-revoked DNSKEY RRset for up to 30 days following the RRSIG(DNSKEY) TTL expiry and recommending that the window be doubled or tripled. [BM] and [NW] argued that a static time window is the wrong approach entirely, and proposed a telemetry-driven alternative in which the revoked key remains published until RFC 8145 signaling or passive root server telemetry indicates that reliance on the old trust anchor has dropped below a defined threshold.

ICANN org Analysis:

The behavior of RFC 5011-compliant resolvers during the revocation phase is straightforward: when a resolver observes the REVOKE bit set on a trust anchor, it revokes that key immediately. It does not require an extended window to complete that action: revocation is a one-time event triggered by observation of the bit. The 70-day window is therefore not primarily sized to ensure compliant resolvers have sufficient time to process the revocation. Rather, it provides a publication period long enough that resolvers which have cached a prior view of the DNSKEY RRset will, upon cache expiry, query the root zone and observe the revoked key before it is removed. Given that DNSKEY TTLs and RRSIG validity periods in the root zone are measured in days rather than weeks, 70 days provides substantial margin above any plausible cache lifetime. ICANN org does not consider the 70-day window insufficient on the basis of the caching concern raised.

The proposed telemetry-driven approach of holding the revoked key until signaling data indicates reliance has dropped is noted, but the operational experience from the 2018 KSK rollover gives reason for caution. During the revocation phase of that rollover, RFC 8145 signaling initially reported that reliance on the old key had declined, but query traffic crept back up following apparent revocation, suggesting that signaling data alone may not provide a reliable or stable basis for a removal decision and that apparent convergence can be transient. Basing the removal trigger on a threshold that has demonstrated instability in practice would introduce uncertainty into what is designed to be a predictable, well-sequenced operation.

ICANN org expects to gain additional operational insight from the revocation phase of the current KSK rollover, before the algorithm rollover begins. That experience, including observed query traffic patterns, RFC 8145 signaling behavior, and any recurrence of the post-revocation uptick phenomenon, will inform the operational execution of Phase FF. The 70-day window will be maintained as proposed, with the understanding that Phase FF timing can be adjusted at a quarter boundary should operational data from the current rollover's revocation phase indicate that adjustments are warranted before Phase FF of the algorithm rollover is executed.

3.6 Implementation Timeline

Comment Summary:

[SSAC] raised three concerns about the proposed timeline. First, it questioned whether Phase AA needs to begin in Q2/2027, noting that the personnel, facilities, and procedures relevant to Phase AA will have been exercised during the October 2026 KSK rollover, and suggesting Q4/2026 as a viable alternative start date. Second, it found no technical explanation for why Phase EE is planned to last approximately two years, given that the RFC 5011 mandatory hold-down period is 30 days, and suggested that Phase EE's exit could be triggered by a telemetry threshold rather than a fixed time limit. Third, it noted the absence of defined success criteria or specific thresholds for triggering phase extensions under the plan's phase scheduling provisions.

ICANN org Analysis:

On the Phase AA start date, the proposed timing follows the same sequencing approach described in the Proposal for Future Root Zone KSK Rollovers [2019] and reflects the operational realities of conducting key signing ceremonies at quarterly intervals, with a single well-defined root zone change per quarter. Notably, the ZSK size reduction is designed to follow the revocation phase of the current KSK rollover. This sequencing is deliberate: it avoids compressing multiple root zone changes into a single quarter, which would increase operational complexity and the risk of error.

ICANN org acknowledges the SSAC's suggestion that bringing Phase AA forward is a reasonable consideration. However, the algorithm rollover introduces elements genuinely novel in ICANN org's operational experience, most significantly the generation of an ECDSA KSK, which will be the first ECDSA key signing ceremony ICANN org has conducted for the root zone. This requires updated ceremony scripts, revised Key Signing Key Policy and Key Management Framework documentation, and validation of ECDSA operations within the HSM environment. This preparation is distinct from what the current KSK rollover exercises and requires adequate lead time following the conclusion of current operations. This readiness work is already underway, and ICANN org expects to be ready to execute Phase AA in Q2/2027.

On the Phase EE duration, the two-year window is consistent with prior KSK rollovers and is designed to accommodate the long tail of trust anchor updates that do not occur via RFC 5011. While RFC 5011 enables automated updates for resolvers that implement and have it configured, a portion of the validating resolvers relies on statically configured trust anchors requiring manual operator action or vendor software releases, processes that may operate on timescales of months to years. The two-year Phase EE window provides time for this broader ecosystem to update. A threshold-based exit trigger, as suggested by SSAC, is noted, but for similar reasons discussed in section 3.5 regarding Phase FF telemetry, ICANN org does not consider resolver signaling data sufficiently stable to serve as a trigger. Notwithstanding this, throughout Phase EE, ICANN org will continue to generate forward transition SKRs on a quarterly basis to allow for forward progression to Phase FF should it be deemed operationally necessary.

On the absence of defined success criteria for phase extension decisions, ICANN org considers this a valid observation. The plan's ability to extend or hold phases at quarter boundaries provides the mechanism for such decisions, and the specific operational criteria that would trigger their use will be defined in ICANN org's implementation documentation.

3.7 TTL Expiration Handling

Comment Summary:

[JX] argued that ICANN routinely requires documentation of TTL-expiration waiting periods in TLD-level DNSSEC transition plans, and that no equivalent provision appears in the current proposal. [DS] raised the same concern independently.

ICANN org Analysis:

The TTL-expiration waiting periods required in TLD-level DNSSEC transition plans reflect the fact that TLD operators can design a rollover to occur within days, which is relatively significant compared to the TTLs on their DNSKEY and related records. The root zone operates under different conditions. Every phase of the algorithm rollover is structured around a calendar quarter of approximately 90 days, a duration that exceeds even the longest root zone TTL by more than an order of magnitude. TTL expiration is therefore implicitly guaranteed by the quarterly phase structure rather than requiring explicit documentation as a discrete step. No change to the proposal is necessary on this basis.

3.8 Resolver Readiness, Monitoring, and Operator Support

Comment Summary:

[JI] argued that edge cases involving older systems and environments with improperly updated trust anchors represent the most likely source of early problems, and called for improved visibility into validation failures and fallback patterns during the double-signing phase. [NHN] recommended public dashboards, deployment playbooks, reference configurations, and containerized testbeds. [NHN] and [GE] expressed concern about particular risks in developing regions, arguing that constrained infrastructure and legacy systems could make the double-signing phase especially risky, and called for targeted outreach and documented manual fallback protocols.

ICANN org Analysis:

ICANN org notes that the SSAC's assessment of ecosystem readiness provides the most comprehensive and authoritative view of this question. Algorithm 13 (ECDSA P-256) is a mandatory implementation algorithm under RFC 8624 and RFC 9904, surpassed Algorithm 8 (RSA/SHA-256) globally in deployment as of April 2024, and is supported by all major open-source and commercial DNS resolvers. The broad deployment baseline substantially reduces the risk of the resolver compatibility failures described by submitters.

Monitoring of the root zone signing and validation environment is an ongoing operational activity, and the plan is explicitly designed to allow phase timing to be adjusted at quarter boundaries in response to conditions that diverge from expectations. The concerns raised regarding visibility into validation failures and truncation rates during double-signing are consistent with the monitoring posture already anticipated by the plan.

ICANN org takes note of the specific concerns raised regarding developing regions and under-resourced operators. Communications and outreach will be developed to ensure that rollover communications address the needs of operators in regions where infrastructure constraints may affect transition readiness. In addition, ICANN org will make available tools replicating the planned phase transitions to support resolver vendors and developers in assessing and confirming software and configuration readiness ahead of the transition.

3.9 Document Quality, Decision Rationale, and KSR Composition

Comment Summary:

[MS] and [DS] argued that the proposal documents design choices without explaining the rationale behind them, making it difficult to evaluate critical decisions or assess alternatives. [MS] additionally raised the absence of per-phase KSR composition details, and several editorial concerns including the lack of section numbers, page numbers, and a state-transition diagram, and inconsistent use of the term "Slot." [JX] noted that the algorithm associated with "KSK-2024" is not stated, and argued that the use of 1536 bits should be explicitly justified.

ICANN org Analysis:

This Public Comment response serves as the primary record of rationale for the key design decisions in the proposal. The analyses in sections 3.1 through 3.9 address the substantive concerns raised about decision transparency, including the ZSK size selection, the rejection of the ZSK-first alternative, the purpose and structure of Phase DD, and the sizing of the Phase EE and Phase FF windows, and are intended to be read alongside the proposal as the complete basis for the rollover plan.

Per-phase KSR composition details (specifically the keys and signatures comprising each SKR set at each ceremony) are operational rather than policy-level documents. They will be documented in the Key Signing Ceremony procedures and supporting operational materials that accompany each ceremony, consistent with how such details are handled for existing KSK rollover ceremonies.

Section 4: Next Steps

ICANN org thanks all participants in this proceeding for the quality and depth of engagement. Having considered the feedback received, ICANN org intends to proceed with the Root Zone KSK Algorithm Rollover as described in the proposal. The Public Comment proceeding has surfaced a number of areas where additional documentation and pre-execution work will strengthen the operational basis for the rollover, and the following next steps reflect those commitments.

- Define and publish phase transition metrics. The plan provides for phase extensions and holds at quarter boundaries; the specific operational criteria and thresholds that would trigger such adjustments will be defined and published. This directly addresses the

concern raised by SSAC that the absence of defined success criteria limits the practical utility of those provisions.

- Distribute software. ICANN org will make available software that simulates the planned phase transitions, enabling resolver vendors and developers to validate software and configuration readiness, and to support further analysis in support of the implementation of this plan. ICANN won't operate a public test bed due to the confusion as to its use and applicability.
- Conduct operator outreach. ICANN org will develop and distribute rollover communications targeted at the operator community, with specific attention to operators in developing regions and those relying on statically configured trust anchors, ahead of each major phase transition. ICANN org also notes the lack of responses from resolver implementers and operators and will seek direct feedback from those communities.

In parallel, ICANN org will monitor the rollover and revocation phases of the current KSK rollover for operational lessons relevant to the execution of Phase FF revocation.