SAC133
SSAC Comments on Proposed Root KSK Algorithm Rollover

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
10 April 2026

Preface

This is a public comment to the ICANN organization from the ICANN Security and Stability Advisory Committee (SSAC) in response to a call for comments for the Proposed Root Key Signing Key (KSK) Algorithm Rollover.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any withdrawals included at the end of the document.

1 Introduction

The ICANN Security and Stability Advisory Committee (SSAC) thanks the ICANN organization (org) for the opportunity to comment on the proposal for the Domain Name System (DNS) root zone Key Signing Key (Root KSK) algorithm rollover.[1] The SSAC supports the overarching goal of the proposal to transition the Root KSK from RSA with SHA-256 (Algorithm 8) to ECDSA P-256 with SHA-256 (Algorithm 13),[2] and commends ICANN and the Root Zone Maintainer (RZM) for the care and rigor reflected in this work. The SSAC recognizes this proposal as a significant step toward addressing Recommendation 23 of the Second Security, Stability, and Resiliency (SSR2) Review Final Report, adopted by the ICANN Board in July 2021.[3]

In this comment, the SSAC provides both general and specific observations intended to affirm the proposal's technical soundness and offer targeted recommendations on the RSA Zone Signing Key (ZSK) size reduction and the implementation timeline.

2 General Comments

The SSAC supports the transition from RSA with SHA-256 (Algorithm 8) to ECDSA P-256 with SHA-256 (Algorithm 13) as the cryptographic algorithm for the RootKSK. The root zone has relied on RSA-based algorithms since DNSSEC signing began in 2010. The algorithm did not change during the first KSK rollover in 2018 or during the second rollover currently underway and scheduled to complete in October 2026. Establishing a clear and predictable process for algorithm transitions is essential to the long-term security of the root zone, and the SSAC observes that the proposal addresses the Recommendation 23 of the SSR2 Review accordingly.

The SSAC notes that the proposal builds upon the Root Zone DNSSEC Algorithm Rollover Study published by ICANN in May 2024, which assessed resolver and authoritative server support for alternative algorithms, analyzed rollover methodologies, and evaluated operational risks.[4] The SSAC finds that the proposal implements the study's recommendations. The SSAC

[1] ICANN. "Proposed Root KSK Algorithm Rollover." Public Comment. https://www.icann.org/en/public-comment/proceeding/proposed-root-ksk-algorithm-rollover-03-02-2026.
[2] IANA. "Domain Name System Security (DNSSEC) Algorithm Numbers." https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml.
[3] *Second Security, Stability, and Resiliency (SSR2) Review Team Final Report*. ICANN, 2021. https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf.
[4] *Root Zone Algorithm Rollover Study*. ICANN, 2024. https://www.icann.org/en/system/files/files/root-zone-algorithm-rollover-study-23may24-en.pdf.

also notes that this proposal is consistent with the SSAC's prior work on DNSSEC key rollover, including SAC063, SAC073, SAC102, and SAC108.[5, 6, 7, 8]

The SSAC encourages ICANN to proceed with this rollover. Specific comments on the proposal's methodology, timeline, and operational readiness follow.

3 Specific Comments on the Proposal

3.1 Comments on Algorithm Selection and Rollover Methodology

The SSAC supports the selection of ECDSA P-256 with SHA-256 (Algorithm 13) as the successor algorithm. This selection is consistent with the criteria established by the 2024 Rollover Study: the algorithm is standardized through the Internet Engineering Task Force (IETF) and is designated as a mandatory implementation algorithm for both signing and validation under RFC 8624 and RFC 9904.[9, 10] Algorithm 13 has been adopted by numerous top-level domains, including .com, .net, and .gov, and is widely supported across major open-source and commercial DNS software, including BIND, Unbound, Knot Resolver, and PowerDNS Recursor.

The SSAC supports the use of the double-signing approach as an appropriate methodology for this algorithm transition. Signing the root zone with both the incumbent RSA key and the new ECDSA key during the transition period avoids the need to pre-publish the new trust anchor, thereby maintaining compliance with the mandatory algorithm rules in RFC 6840.[11] This approach is consistent with guidance in SAC063 and SAC073, which emphasized the importance of a cautious, staged transition methodology for root zone key changes.[12, 13]

---

[5] *SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone*. ICANN Security and Stability Advisory Committee (SSAC), 2013. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-063-en.pdf.

[6] *SAC073: SSAC Comments on Root Zone Key Signing Key Rollover Plan - Design Teams Draft Report*. ICANN Security and Stability Advisory Committee (SSAC), 2015. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-073-en.pdf.

[7] *SAC102: SSAC Comment on the Updated Plan for Continuing the Root KSK Rollover*. ICANN Security and Stability Advisory Committee (SSAC), 2018. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-102-en.pdf.

[8] *SAC108: SSAC Comments on the IANA Proposal for Future Root Zone KSK Rollovers*. ICANN Security and Stability Advisory Committee (SSAC), 2020. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-108-en.pdf.

[9] Wouters, P. and O. Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC", RFC 8624, DOI 10.17487/RFC8624, June 2019, https://www.rfc-editor.org/info/rfc8624.

[10] Hardaker, W. and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process", RFC 9904, DOI 10.17487/RFC9904, November 2025, https://www.rfc-editor.org/info/rfc9904.

[11] Weiler, S., Ed., and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, https://www.rfc-editor.org/info/rfc6840.

[12] *SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone*.

[13] *SAC073: SSAC Comments on Root Zone Key Signing Key Rollover Plan - Design Teams Draft Report*.

The SSAC supports the proposal's inclusion of backout signed key responses (SKRs) for each rollover phase and the Flexible Phase Scheduling provisions that allow any phase to be extended across multiple quarters. These provisions constitute appropriate operational safety valves consistent with the lessons of the 2018 KSK rollover. However, the SSAC notes that the current plan lacks success criteria for each phase or specific thresholds for significance or other relevant variables that would prompt a schedule extension. Without these parameters, there is no objective basis for determining when an extension is necessary or when it is safe to resume the rollover. The use of distinct phase identifiers (AA through HH) to differentiate this algorithm rollover from prior non-algorithm rollovers is a sensible operational convention.

3.2 Comments on the RSA ZSK Size Reduction

Prior to the algorithm transition, the proposal reduces the root zone's RSA ZSK from 2048 to 1536 bits — a reduction the SSAC believes warrants careful explanation. The SSAC's assessment is that the reduction is operationally advisable to navigate the current network environment, but recommends that the final implementation plan formalize this as a justified, strictly time-bound exception to current cryptographic best practices that establishes no precedent for future operations.

During a double-signing algorithm rollover, root zone referral responses, DNSKEY answers, and NXDOMAIN responses must simultaneously carry signatures for two algorithms. The 2020 DNS Flag Day established 1232 bytes as the default maximum User Datagram Protocol (UDP) buffer size used by resolvers. With double-signing and a 2048-bit RSA ZSK, many root server responses would exceed 1232 bytes, triggering truncation and Transmission Control Protocol (TCP) retransmission at a scale that affects resolution performance to a non-negligible degree. Reducing the RSA ZSK to 1536 bits permits almost all responses to remain under the 1232-byte threshold.

The SSAC acknowledges that the US National Institute of Standards and Technology (NIST) recommends 2048-bit RSA keys as the minimum for security. A 1536-bit RSA key provides approximately 96 bits of security,[14] which is significantly below the 2048-bit key's security level of 112 bits.[15] For cryptographic material expected to remain in use for years or decades, 128 bits of security (as provided by the post-rollover ECDSA keys) is a commonly targeted goal.[16]

[14] Calculated based on the equivalence formula for key strengths defined in National Institute of Standards and Technology (NIST), *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program*, Annex D – Approved sensitive security parameter generation and establishment methods, Section D.B – Strength of SSP Establishment Methods. Applying the specified formula (Equation 1) for an RSA key length of L = 1536 yields an equivalent symmetric key strength of approximately 96.6 bits.
[15] Barker, Elaine. *Recommendation for Key Management: Part 1 - General*. Table 2: Comparable security strengths of symmetric block cipher and asymmetric-key algorithms. NIST SP 800-57pt1r5. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5.
[16] Federal Office for Information Security. "BSI TR-02102-1 'Cryptographic Mechanisms: Recommendations and Key Lengths' Version: 2026-01."

However, the RSA ZSK affected by this reduction is in a fundamentally different position. Because the ZSK public component remains private between ICANN and the RZM until it is pre-published in the root zone, each ZSK can be subjected to public cryptanalytic scrutiny for approximately 110 days per key (a 90-day active signing quarter, flanked by 10-day pre- and post-publication slots). This strictly limits an attacker's window of opportunity, making it computationally infeasible to break a 1536-bit key before it is retired and removed from the zone.[17] Furthermore, the specific 1536-bit RSA ZSK key size is expected to remain in effect only for the projected three-year duration of the algorithm rollover period from Phase AA to Phase FF.

To properly justify this time-bound accommodation, the SSAC encourages ICANN org to include a cryptographic estimate of the computational cost and time required to break a key of this size within its short operational window in the final implementation plan.

A public comment submitted to this proceeding proposes avoiding the ZSK size reduction by instead rolling the ZSK to Algorithm 13 before transitioning the KSK.[18] As that comment itself correctly notes, this approach would constitute a violation of the mandatory algorithm rules in RFC 6840.[19] A draft specification that would permit this approach has not been adopted by the IETF Domain Name System Operations (DNSOP) working group.[20] The SSAC concurs with the proposal's rejection of this alternative.

The SSAC supports the 1536-bit RSA ZSK reduction as operationally advisable and adequate for the purposes of this specific plan, but emphasizes that a downgraded key should not remain in service any longer than strictly necessary. This reinforces the SSAC's comments regarding the implementation timeline in Section 3.3 below.

3.3 Comments on the Implementation Timeline

The proposal spans approximately four years, from ECDSA KSK generation in Q2/2027 (Phase AA) to final deletion of RSA key material in Q3/2030 (Phase HH). The SSAC finds the overall phased structure appropriate, but questions whether the full four-year duration is necessary. The

---

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html?nn=132646.

[17] This assumes a publicly observable attack window. However, in a scenario where a covert attacker obtains the ZSK public key prior to root zone pre-publication, the effective window could extend to approximately 193 days. Even so, less than a doubling of available attack time does not alter the conclusion that breaking a 1536-bit key within even the extended window remains computationally infeasible.

[18] StJohns, Michael. "Submission." 12 February 2026. https://www.icann.org/en/public-comment/proceeding/proposed-root-ksk-algorithm-rollover-03-02-2026/submissions/stjohns-michael-12-02-2026.

[19] Weiler and Blacka, "Clarifications and Implementation Notes for DNS Security (DNSSEC)."

[20] Huque, S., P. Thomassen, V. Dukhovni, D. Wessels, and C. Elmerot. "Multiple Algorithm Rules in DNSSEC." Work in Progress, Internet-Draft, Draft-Huque-Dnsop-Multi-Alg-Rules-07, 20 October 2025, https://datatracker.ietf.org/doc/draft-huque-dnsop-multi-alg-rules/.

SSAC notes that a shorter rollover period (achieved through shortening the phase EE period, as discussed below) would also reduce the total time the 1536-bit RSA ZSK is in active use, which is a relevant security consideration in light of the observations in Section 3.2. Additionally, while DNSSEC does not face the same post-quantum urgency as other protocolsthat are already deploying post-quantum cryptography today, avoiding prolonged use of a short-sized RSA ZSK during this time of transition would reflect sound planning on ICANN's part.

Phase EE (Key Publication and Double Signing) is planned to last approximately two years. During this period, both the incumbent RSA key and the new ECDSA key are simultaneously present in the root zone, allowing resolvers to update their trust anchors via RFC 5011 automated rollover.[21] However, the SSAC finds no technical explanation in the proposal for why two years are required for a process with a mandatory hold-down period of 30 days. The SSAC requests that the final implementation plan include an explicit operational justification for this extended duration. The SSAC suggests evaluating whether it would be more technically defensible to set the duration of Phase EE to a threshold rather than a strict time-based limit. If available telemetry from the 2018 rollover and the ongoing 2025 rollover can establish a clear metric, the transition out of Phase EE could be triggered by meeting that threshold. The SSAC notes that because the implementation plan already provides mechanisms for timeline extensions if necessary, a threshold-based approach may allow for a faster Phase EE if the ecosystem is ready, while preserving security and stability if it is not.

The proposal targets Q2/2027 for Phase AA (ECDSA KSK generation), approximately six months after the October 2026 KSK rollover is expected to be completed. Phase AA involves only ECDSA KSK generation and secure storage, with no changes to the root zone. The SSAC notes that the personnel, facilities, and procedures required for Phase AA will have just been exercised and validated through the October 2026 rollover, and questions why Q4/2026 could not serve as a viable start date.

3.4 Comments on Operational Readiness

The SSAC supports the continued reliance on RFC 5011[22] as the primary mechanism for resolver operators to adopt the new ECDSA KSK. The 2024 Rollover Study found that Algorithm 13 is a mandatory implementation algorithm under current DNSSEC standards and is widely supported across the resolver ecosystem.

The SSAC finds that broader ecosystem readiness for the ECDSA P-256 transition is well-established. Algorithm 13 is a mandatory implementation algorithm under RFC 8624[23] and

[21] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, https://www.rfc-editor.org/info/rfc5011.
[22] StJohns, "Automated Updates of DNS Security (DNSSEC) Trust Anchors."
[23] Wouters and Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC."

RFC 9904,[24] and its deployment reflects that status. As of April 2024, Algorithm 13 deployment surpassed Algorithm 8 globally and has continued to grow, while Algorithm 8 has plateaued. The deployment data is consistent with operational experience: Algorithm 13 is actively deployed by major top-level domains (including .com, .net, and .gov) with no reported issues, and SIDN's completed algorithm rollover for .nl in 2023 concluded that Algorithm 13 is widely supported across the resolver ecosystem.[25] Algorithm 13 is supported by major open-source DNS resolvers[26] and commercial DNS platforms. Furthermore, ICANN's operational environment has been updated to support ECDSA, with Thales Luna G7 Hardware Security Modules confirmed within the parameters of the DNSSEC Practice Statement for the Root Zone KSK Operator.[27]

The SSAC notes that the proposal's Flexible Phase Scheduling provisions provide an intended safety net for unanticipated compatibility issues. If significant groups of legacy resolvers are identified during Phases CC or DD as failing to correctly process ECDSA signatures, the schedule can be extended while remediation is pursued. However, as noted in Section 3.1, the absence of defined success criteria and specific thresholds limits the practical utility of this mechanism.

4 Acknowledgments, Disclosures of Interest, and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgements section lists the SSAC members, outside experts, and ICANN staff who co-authored or contributed directly to this particular document or who provided reviews. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this report. The Withdrawals section identifies individuals who have recused themselves from the discussion of the topic with which this report is concerned. Except for members listed in the Withdrawals section, this document has the consensus approval of all of the members of SSAC.

4.1 Acknowledgments

The committee wishes to thank the following SSAC members and ICANN staff for their time, contributions, and review in producing this report.

[24] Hardaker and Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process."
[25] Ubbink, Stefan, Jeroen Bulten, and Niek Willems. "Looking Back at .nl's Algorithm Rollover." SIDN. https://www.sidn.nl/en/news-and-blogs/looking-back-at-nls-algorithm-rollover.
[26] *SAC132: The Domain Name System Runs on Free and Open Source Software (FOSS)*. Table 5: Commonly Used FOSS Systems for DNS Server Applications, ICANN Security and Stability Advisory Committee (SSAC), 2025. https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac132-25-09-2025-en.pdf.
[27] Root Zone Key Signing Key Operator Policy Management Authority. *DNSSEC Practice Statement for the Root Zone KSK Operator, 8th Edition*. 2025. https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20250414.html.

SSAC Members
Maarten Aertsen
Nabil Benamar
Wes Hardaker
Russ Housley
Geoff Huston
Warren Kumari
John Levine
Danny McPherson
Peter Thomassen
Laurin Weissinger
Rick Wilhelm

ICANN Staff
Daniel Gluck
Michael Puckett
Carlos Reyes
Danielle Rutherford (Editor)
Kathy Schnitt

4.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest at the time of publication are available at: https://www.icann.org/en/ssac/members/archive/25-01-2026.

4.3 Withdrawals

There were no withdrawals.