# Public Comment Summary Report

## Draft Report of the Root Zone DNSSEC Algorithm Rollover Study

**Open for Submissions Date:**
Thursday, 19 October 2023

**Closed for Submissions Date:**
Monday, 4 December 2023

**Summary Report Due Date:**
Monday, 18 December 2023

**Category:** Technical

**Requester:** Other

**ICANN org Contact:** james.mitchell@iana.org**,** kim.davies@iana.org

**Open Proceeding Link:** https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023

**Outcome**:
The design team received a total of seven submissions from groups, organizations, and individuals. The submissions provided input on all aspects of the report and identified areas requiring further analysis and consideration. The design team will soon begin a thorough review of the Public Comment submissions for the final publication of their report.

## Section 1: What We Received Input On

The Root Zone Domain Name System Security Extensions (DNSSEC) Algorithm Rollover Design Team sought community input and comments on their draft report. The design team was tasked with two key tasks:

- providing guidance on how to select an algorithm for the root zone, and
- investigating how a rollover could be conducted.

**The team specifically sought feedback on their recommendations and whether the rollover methods were appropriate.** The exact timing of an algorithm rollover and the design of detailed operational plans were out of scope for the design team.

## Section 2: Submissions

**Organizations and Groups:**

| Name | Submitted by | Initials |
|---|---|---|
| Verisign, Inc. | Burt Kaliski | Verisign |
| Registries Stakeholder Group | | RySG |
| Cloudflare | Joseph Abley | Cloudflare |
| Root Server System Advisory Committee | Jeff Osborn | RSSAC |

**Individuals:**

| Name | Affiliation (if provided) | Initials |
|---|---|---|
| George Michaelson | Asia Pacific Network Information Centre (APNIC) | Michaelson |
| Julius Kirimi | African Regional At-Large Organisation (AFRALO) | Kirimi |

## Section 2a: Late Submissions

At the ICANN organization's (org) discretion, the org accepted late submissions that were appended to this summary report.

**Organizations and Groups:**

| Name | Submitted by | Initials |
|---|---|---|
| ICANN Security and Stability Advisory Committee | Steve Sheng | SSAC |

# Section 3: Summary of Submissions

**Response Sizes**

- Consider local root and reduction of traffic to root servers (Cloudflare)
- Consider recent operational experience demonstrating undesired resolver behavior during recent algorithm rollovers (Verisign)
- Consider the option to reduce the number of glue records returned in referrals (Verisign)

**Algorithm Selection**

- Consider whether RFC 8624 analysis is sufficient (SSAC)
- Consider quantitative thresholds for all algorithm selection requirements (SSAC)
- Prepare for post-quantum cryptography (Verisign)

**Implementation**

- Pre-publication conflicts with RFC 6840 (SSAC)
- Consider documenting the potential for downgrade attacks during dual signing (SSAC)

**Testing and Measurement**

- Define measurements before, during, and after the algorithm rollover (Michaelson)
- Consider access to test environments and test data (Kirimi)

**Hardware**

- Detail the consequences of downgrading Federal Information Processing Standards (FIPS)-140 compliance (Michaelson)
- Ensure new hardware security modules (HSMs) are in place before an algorithm rollover (Michaelson)

**Report**

- Consider re-ordering the recommendations for clarity (RySG)
- Provide clarification where further work is required (RySG)
- Provide general improvements for the reader (RySG)

**Other**

- Consider other uses of the root zone trust anchor (Verisign)

## Section 4: Analysis of Submissions

The following is a preliminary analysis for several selected comments from the submissions. All submissions from this public proceeding will be considered by the design team for incorporation into their final report.

| | |
|---|---|
| Consider the option to reduce the number of glue records returned in referrals | A reduction in the number of glue records or adoption of compression-friendly host names will reduce packet sizes, which may improve overall performance both during and before or after a rollover. |
| Consider quantitative thresholds for all algorithm selection requirements. | The decision to introduce or rollover the key used to sign the root zone must be informed by quantitative analysis. An algorithm rollover should not have a negative impact greater than that of a traditional rollover. |
| Prepare for post-quantum cryptography | The report recommends the algorithm is assessed periodically, approximately every three years in conjunction with a planned rollover cadence. The community should progress the development of post quantum algorithms before they are needed in the root zone. |
| Consider pre-publication conflicts with RFC 6840 | Initial testing has shown that the tested validators accept any valid path, consistent with the recommendations in 5.11, however we agree that updates to the standards are necessary. |
| Define measurements necessary before, during, and after the algorithm rollover | The development of specific measurements was deferred to the creation of a detailed operational plan. We will revisit this decision. |
| Consider access to test environments and test data. | Test environments should be made available to facilitate the wider testing of resolvers, |

| | |
|---|---|
| | especially for vendors of closed-source or proprietary systems. |
| Detail the consequences of downgrading FIPS-140 compliance. | The Internet Assigned Numbers Authority (IANA) has been preparing a plan to replace the current line of HSMs after the vendor announced their intention to exit the line of business. That project includes a detailed analysis of the FIPS-140 standards. Further information on that plan will be announced early 2024. |

## Section 5: Next Steps

All submissions from this public proceeding will be considered by the design team for incorporation into their final report. The design team will resume their meetings in January 2024 and are expected to publish their report in the first half of 2024.

SSAC
ICANN Security and Stability Advisory Committee

8 December 2023

Subject: SSAC2023-22: SSAC's Comment on Root Zone Algorithm Rollover Study Draft Report

The SSAC has reviewed a draft report of the design team concerning DNSSEC algorithm rollover in the root zone.[1] We offer these comments as part of the associated Public Comment process.

Overall, we find the report to be both well-informed and informative. We think the recommendations of the report are in-scope, appropriate, and well-supported.

We suggest that it would be useful for future work around this topic to consider opportunities to update the published guidance from the IETF that relates to algorithm rollover. A careful focus on algorithm rollover in the root zone would likely suggest improvements to existing guidance that are important to record. We encourage those engaged in algorithm selection and the implementation of a future algorithm rollover to look for opportunities to facilitate that. We offer four examples below.

1. As the report recommends, future selection of an incoming algorithm must be based in part on the availability of that algorithm among the relying parties who consume its corresponding signatures. When selecting an algorithm, it might be useful to consider whether the guidance provided in RFC 8624[2] is sufficient; if the root zone algorithm selection process includes additional considerations or finds some other framework that is useful in the selection of a suitable algorithm, we think that updating RFC 8624 would be useful.

2. While the report identifies specific thresholds for some of the identified requirements for selecting a successor algorithm, many of the requirements have no corresponding quantitative thresholds. This seems like an omission. We think clear, quantifiable criteria are important to define, and if they are not defined in this study, we think this study ought to recommend subsequent studies do so.

3. In the case where the incoming key introduces an algorithm not previously used in the zone, pre-publication of the corresponding trust anchor is not currently allowed by RFC 6840[3] section 5.11. This seems like a problem that the study should recognise, especially given draft recommendation 3. The study should recommend that work be done to update the standards through the appropriate IETF process.

4. The advice to dual-sign during an algorithm rollover is based in part on the avoidance of downgrade attacks in the case where an outgoing algorithm is considered to be less strong than an incoming algorithm. In the case of an algorithm rollover where the incoming and outgoing algorithms are of comparable strength, and the change of algorithm is motivated by other factors

[1] Root Zone Algorithm Rollover Study (Draft), Design Team Report, 19 October 2023, https://itp.cdn.icann.org/en/files/domain-name-system-security-extensions-dnssec/draft-report-root-zone-dnssec-algorithm-rollover-study-19-10-2023-en.pdf
[2] https://www.rfc-editor.org/rfc/rfc8624
[3] https://www.rfc-editor.org/rfc/rfc6840

such as response size, it is not clear that this advice is useful. We think a root zone algorithm rollover provides a good opportunity to document these considerations and revisit ideas of best practice.

We thank the design team for their work and look forward to the next steps in the evolution of DNSSEC deployment.

Rod Rasmussen
Chair, ICANN Security and Stability Advisory Committee