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