Registries Stakeholder Group Statement

Draft Report of the Root Zone DNSSEC Algorithm Rollover Study

Date statement submitted[1]: 1 December 2023

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

Background[2]

The Root Zone DNSSEC Algorithm Rollover Design Team seeks 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 seeks feedback on their recommendations and whether the rollover methods are appropriate. The exact timing of an algorithm rollover, recommendations on specific algorithms, and the design of detailed operational plans was out of scope for the design team.

Documents

- Draft Report of the Root Zone DNSSEC Algorithm Rollover Study (pdf, 851.7 KB)

Registries Stakeholder Group Comment

The Registries Stakeholder Group (RySG) appreciates the opportunity to comment on the Draft Report of the Root Zone DNSSEC Algorithm Rollover Study.

Overall, the RySG is supportive of the general concept of the DNSSEC Algorithm Rollover to improve the cryptographic algorithm used in the signing of the DNS root zone. While the RySG has confidence in the current algorithm, we also recognize the need to avoid complacency and to adopt a stronger algorithm before it is strictly needed. Given that the signing algorithm has not previously been changed, the selection and rollover process is of particular importance. We appreciate the Design Team's attention to security and stability considerations, which are evident throughout the report. We particularly note the proper attention given to operational considerations such as the impact to resolvers and message size considerations. Additionally, we expect that the knowledge and experience gained from this activity will be useful to Registry Operators (and Registry Service Providers) to help preserve and maintain the security and stability of their respective authoritative DNS services.

[1] This is a copy of the text submitted via the ICANN Public comment platform.
[2] Background: intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.

Regarding the content in the Study, the RySG offers the following specific comments:

- In the Introduction, there is a statement that: "...some recommendations may be intentionally vague, with the expectation that they will be refined through subsequent work". It would be helpful to the reader if such Draft Recommendations, which are targeted by the authors for subsequent work, would be more clearly identified.
- The sequencing and grouping of the Draft Recommendations could be improved. As an example, Draft Recommendation 3 and Draft Recommendation 16 appear to presuppose a particular decision on Draft Recommendation 14. This becomes clear when looking at them side-by-side:
    - Draft Rec 3: The publication of new trust anchors should happen significantly before the introduction of the new algorithm's DNSKEYs in the root zone.
    - Draft Rec 16: Trust anchors using new algorithms should be pre-published using the existing trust anchor distribution mechanisms as done for non-algorithm rollovers.
    - Draft Rec 14: After selecting the future algorithm, it should be decided whether to begin the rollover process with a pre-publication of the trust anchor (suitable specification updates allowing) or whether to avoid pre-publication. To inform the decision, it should be assessed how double signing the root zone with the new algorithm would impact root server operators, resolver operators, and potential (e.g., packet flood) attack victims, and whether pre- publication benefits outweigh the risks.
- Overall, it would be helpful to make the target audience more clear. At present, the document is oriented toward DNS experts, which is not necessarily a problem. However, the closest that the document comes to alerting the reader is the last line of the executive summary, which describes the terminology.
- A minor item is that the document would benefit from additional footnotes to support various statements. As an example, consider these paragraphs from Section 3, where we inserted "**FN**" to indicate suggested footnotes:

The DNS root zone was signed in 2010 using RSA/SHA-256. **FN** The first KSK rollover did not change the DNSSEC algorithm, keeping RSA/SHA-256 and the same 2048-bit key size. **FN** Changing the DNSSEC algorithm requires the introduction of a new DNSKEY that uses an algorithm different from what is currently present in the DNSKEY RRset, followed by the removal, possibly after revocation, of the incumbent algorithm.

Verisign, in its capacity as the root zone maintainer, changed the key size of the ZSK from 1024-bit to 2048-bit on 1 October 2016. **FN** While there was a noticeable change of larger signatures and DNSKEY sets, this was not a DNSSEC algorithm change. **FN**

Summary of Submission:

Overall, the Registries Stakeholder Group (RySG) is supportive of the general concept of the DNSSEC Algorithm Rollover to improve the cryptographic algorithm used in the signing of the DNS root zone. While the RySG has confidence in the current algorithm, we also recognize the need to avoid complacency and to adopt a stronger algorithm before it is strictly needed.