Recommendations Regarding Signing the root-servers.net Zone

The root-servers.net zone was created in 1995 as a new way to name the root name servers. Since then, all the root name servers have been given single-letter names in this zone, such as *k.root-servers.net*. The primary purpose of the root-servers.net zone is to be the authoritative location for root server IP addresses.

The root zone has been signed with DNSSEC since 2010. However, in the design of DNSSEC, only authoritative zone data is signed. Non-authoritative data, and glue data in particular, is not signed. In the root zone, the A and AAAA records conveying the root server IP addresses are non-authoritative and are not signed. It means that DNSSEC can tell you whether or not you got the correct data, but not whether or not you got it from the correct server. In other words, DNSSEC doesn't care *where* data comes *from*, only whether or not it has been modified.

Although the root zone is signed with DNSSEC, the root-servers.net zone is not. This was an intentional decision by the Root DNSSEC Design Team. At the time, it was felt that signing root-servers.net was an extra complication, and not strictly necessary due to the way that DNSSEC is designed to protect DNS "leaf" data – i.e. data requested by end users.

In 2017, the RSSAC published its analysis of the naming scheme for individual root servers,[1] much of which focused on having signed data for root server names and addresses. Although the report does not recommend any changes to the current naming scheme, it does discuss the consequences of signing the root-servers.net zone.

Figure 1 shows the relationship between the root zone, the root-servers.net zone, and which types of data are signed, not signed, and could be signed.

[1] RSSAC028 "Technical Analysis of the Naming Scheme Used For Individual Root Servers," https://www.icann.org/en/system/files/files/rssac-028-03aug17-en.pdf

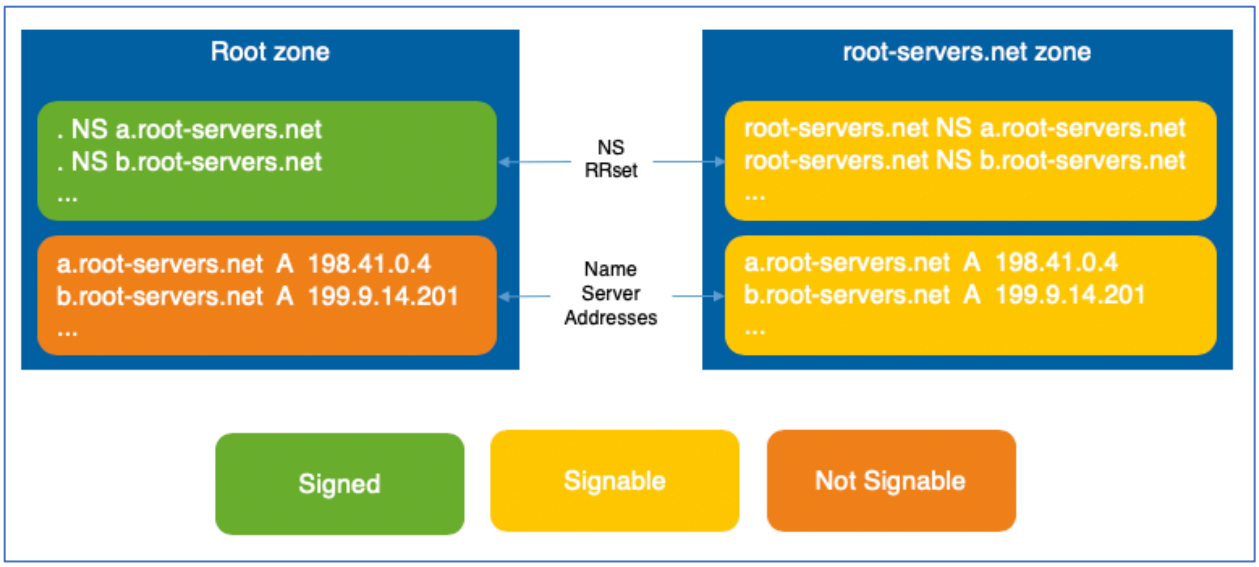

Figure 1. DNSSEC status of data in the root and root-servers.net zones

Signing the root-servers.net zone may be of benefit to validating recursive name servers (aka "validators"). The clear advantage being the ability to ensure that root zone queries go only to real root name server addresses. A validator could detect attempts to alter the IP addresses associated with root server identities and prevent such queries from going to a "spy-in-the-middle."

However, signing the root-servers.net zone also introduces some potential problems. As demonstrated in RSSAC028, the size of a signed priming response can be significantly larger than an unsigned response, depending on the server software in use and the value of the DNSSEC_OK flag in the query. In that report, BIND version 9.10 returned signed priming responses exceeding 3800 bytes. In most networks this results in a UDP message broken into three fragments. It may be undesirable to rely on working fragmentation reassembly for priming queries.

RSSAC028 further showed that other software (Unbound, Knot) generate more reasonably-sized responses.

Another aspect worth considering is how recursive name servers respond to bogus priming responses. In other words, do they actually check signatures and discard data from responses that cannot be validated? Initial investigations by Verisign indicate that some do, and some do not.

Lastly, it may also be worth studying and documenting the interactions of the .net zone between the root zone and the root-servers.net zone. Since root-servers.net is a second-level domain, validation requires the following RRsets:

- net DS record(s)
- net DNSKEY records

- root-servers.net DS record(s)
- root-servers.net DNSKEY records

This effectively changes priming from a simple, single query/response transaction into something more complex, requiring multiple queries to multiple zones.

The RZERC recommends that further research and discussion take place prior to signing the root-servers.net zone. In particular:

1) Understand and document the behavior of authoritative DNS software currently in use by root server operators with respect to a signed root-servers.net zone. This should include, but not necessarily be limited to, the size of a signed priming response. Would this result in a lot of UDP fragmentation? Should root server operators expect to see a significant increase in TCP traffic?

2) Understand and document the behavior of recursive name servers with respect to validating signed priming responses. Do they validate and detect incorrect data? What fraction of priming queries have the DO bit set?

3) Further explore the cost / benefit tradeoffs and risks. Do the risks of redirected query traffic outweigh the risks of increased operational complexity?

4) Foster architectural discussions regarding the intentional design in DNSSEC whereby delegation data is not signed. Is this more important at the root? Should this be considered to apply more widely to all zones?

5) Revisit (probably within RSSAC) the appetite for (and consequences of) giving the root servers names directly in the root zone, such that they become authoritative data and signed by DNSSEC. Perhaps more broadly, should there be a policy that encourages or requires any data on which the root zone depends to be protected by DNSSEC?