Stockholm 2019-03-19

Netnod Statement of Compliance With RSSAC001

Introduction

Netnod is one of the twelve officially recognised operators of the DNS root service for the global Internet. As such, we are expected to adhere to the service expectations for the DNS root service expressed by the Root Server System Advisory Committee (RSSAC) within the Internet Corporation for Assigned Names and Numbers (ICANN) in RSSAC's document RSSAC001[1], which include, by reference, the expectations expressed by the Internet Architecture Board (IAB) expressed in RFC 7720[2].

This is Netnod's statement of compliance with said document.

This statement should be seen as a complement in line with Netnod's letter to the IANA (then part of ICANN) in 2009 through its then subsidiary Autonomica AB[3], in which we expressed our commitment to continue our DNS root service. The letter was sent in cooperation with root server operators the RIPE NCC and WIDE, who sent almost identical letters around the same time, expressing their own commitments.

RSSAC001 is composed of a series of indexed requirements, each followed by an explanation. In the following we respond to each of these requirements. We have tried to make it easy to follow the text by copying relevant parts of RSSAC001, formatting it as follows, and inserting our statements in between the requirements.

> **[X.X.X-X] Bold text: formal requirement text (directly from RSSAC001).**
>
> Normal font: explanation of the formal requirement (directly from RSSAC001).
>
> *Italics and indented: Netnod response statement.*

Find below the relevant parts of RSSAC001, starting at chapter 3.

---

[1] https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf
[2] https://www.rfc-editor.org/info/rfc7720
[3] Autonomica was a direct subsidiary of Netnod from Autonomica's inception in the year 2000 until 2010, when it was formally merged into Netnod in a registered business transaction. In the transaction Netnod willingly assumed any and all responsibilities of its subsidiary, Autonomica, including the operation of the root name service. The merger was done for the sole purpose of ease of administration.

3. Expectations of Root Server Operators

3.1 Infrastructure

[E.3.1-A] Individual Root Server Operators are to publish or continue to publish operationally relevant details of their infrastructure, including service-delivery locations, addressing information and routing (e.g., origin autonomous system) information.

The public availability of this technical information facilitates troubleshooting and general operational awareness of Root Server infrastructure by the Internet technical community. The granularity of this information is limited to the publicly exposed service and at the comfort level of the Root Server Operator.

> *This is published on http://www.root-servers.org/, when clicking the letter "I" in the bottom table.*

[E.3.1-B] Individual Root Servers will deliver the service in conformance to IETF standards and requirements as described in RFC 7720 [4] and any other IETF standards-defined Internet Protocol as deemed appropriate.

> *RFC 7720 specifies the following requirements (quote from RFC 7720):*

> 2. Protocol Requirements
>
> This section describes the minimum high-level protocol requirements. Operative details are documented in [RSSAC001].
>
> The root name service:
>
> - MUST implement core DNS [RFC1035] and clarifications to the DNS [RFC2181].
> - MUST support IPv4 [RFC791] and IPv6 [RFC2460] transport of DNS queries and responses.
> - MUST support UDP [RFC768] and TCP [RFC793] transport of DNS queries and responses.
> - MUST generate checksums when sending UDP datagrams and MUST verify checksums when receiving UDP datagrams containing a non-zero checksum.
> - MUST implement DNSSEC [RFC4035] as an authoritative name service.
> - MUST implement extension mechanisms for DNS (EDNS(0)) [RFC6891].

3. Deployment Requirements

The root name service:

- MUST answer queries from any entity conforming to [RFC1122] with a valid IP address.
- MUST serve the unique [RFC2826] root zone [ROOTZONE].

All of the above are performed as required.

3.2 Service Accuracy

[E.3.2-A] Individual Root Servers will adopt or continue to implement the current DNS protocol and associated best practices through appropriate software and infrastructure choices.

Netnod actively participates in DNS development in relevant IETF working groups, and other fora, such as ICANN (RSSAC, SSAC, and the Board Technical Experts Group), and RIPE (DNS WG), and is an active member of relevant industry consortia, such as DNS-OARC and CENTR. Netnod maintains very good relationships with major DNS vendors, such as the Internet Systems Consortium, NLNet Labs, NIC-CZ, EurID, and more. Netnod takes part in discussions regarding the advancement of the DNS protocol, and remains committed to serving DNS data using relevant and stable DNS software.

[E.3.2-B] Individual Root Servers will serve accurate and current revisions of the root zone.

The root zone content changes regularly although the extent of individual changes is generally small. Note, however, that at the time of this writing, the entire root zone is currently resigned every time it is published, so the DNSSEC signatures (i.e., RRSIG records) change with each new zone.

Netnod remains firmly committed to serving accurate and current revisions of the root zone. Netnod monitors its entire DNS infrastructure, including details of zone versions. DNS extensions TSIG and NOTIFY are employed to ensure zone integrity and timely updates.

[E.3.2-C] Individual Root Servers will continue to provide "loosely coherent" service across their infrastructure.

A set of name servers serving a single zone is said to be "loosely coherent" since although (ordinarily) all name servers in the set serve the same revision of the zone. There will be short intervals following the initial publication of a new revision of the zone in which some servers are observed to serve the now former zone, whilst others serve the newly published zone. These propagation delays are generally either (a) different origin servers in the same anycast cloud giving different answers as changes propagate, (b) different sets of root server infrastructure

(A-M) giving different answers as the zone change propagates. As such the service provided by all 13 root servers by collective inheritance is similarly loosely coherent. Even though this 'loosely coherent' paradigm exists, Root Server Operators will not impose any artificial delays on publishing a new revision of the Root Zone.

> *Netnod does not impose any artificial delays on publication of new versions of the root zone. Our ambition is to always publish the most recent version published by the Root Zone Maintainer.*

[E.3.2-D] All Root Servers will continue to serve precise, accurate zones as distributed from the Root Zone Maintainer.

No Root Server has ever, or will ever, serve a zone that was modified following distribution by the Root Zone Maintainer. In any case, it would be impossible for an individual operator to modify the signed RRsets within the zone, now that it is DNSSEC- signed, without invalidating signatures. A Root Server Operator will not intentionally serve an older zone than current zone provided by the Root Zone Maintainer.

> *In 2009, in the aforementioned open letter to ICANN (as the operators of the IANA function), Netnod (through its then subsidiary Autonomica) made a full and clear statement about Netnod's commitment to serve the root zone data as provided from the IANA, via the Root Zone Maintainer. We hereby reaffirm our statements in that letter. The letter can be found at this URL:*
>
> *https://www.netnod.se/sites/default/files/i-root/autonomica-signed-mri.pdf*

3.3 Service Availability

[E.3.3-A] Individual Root Servers are to be deployed such that planned maintenance on individual infrastructure elements is possible without any measurable loss of service availability.

That is, there ought to be no planned maintenance associated with the operation of any Root Server that would make the corresponding service generally unavailable to the Internet.

> *Netnod operates almost 70 anycast instances, and considers this to be a sufficient guarantee that we are always able to provide service. Since the introduction of anycast, i.root-servers.net has never been generally unavailable and our intention is that it never shall be.*

[E.3.3-B] Infrastructure used to deploy individual Root Servers is to be significantly redundant, such that unplanned failures in individual components must not cause the corresponding service to become generally unavailable to the Internet.

To date there has been no documented example of a simultaneous failure of all Root Servers. The DNS protocol accommodates unavailability of individual Root Servers without significant

disruption to the DNS service experienced by end users. However each root server operator shall employ best efforts in engineering and assign appropriate resources that ensures a commensurate level of component redundancy for the Root Server they operate.

> *All parts of the provisioning chain that are critical to providing the service are duplicated at separate locations, to ensure independent operation. Netnod's anycast service consists of almost 70 instances, all of which operate completely independently of each other.*

[E.3.3-C] Each Root Server Operator shall publish documentation that describes the operator's commitment to service availability through maintenance scheduling and its commitment to the notification of relevant operational events to the Internet community.

> *Netnod always makes prior announcements before any maintenance activity that affects public services.*

3.4 Service Capability

[E.3.4-A] Individual Root Server Operators will make all reasonable efforts to ensure that sufficient capacity exists in their deployed infrastructure to allow for substantial flash crowds or denial of service (DoS) attacks.

Such events might present a significantly greater query load than the observed steady state, and that abnormal load should be accommodated, where possible and within reason, without degradation of service to legitimate DNS clients. Filtering techniques may be employed by Root Server Operators to maintain service to legitimate DNS queries.

> *All Netnod services are designed with significant overprovisioning. Our root service is the most aggressive example of this policy. We have operational experience with successfully providing root service during significant attacks.*

[E.3.4-B] Each root server operator shall publish documentation on the capacity of their infrastructure, including details of current steady-state load and the maximum estimated capacity available.

A root server operator might choose to publish its maximum estimated capacity in high-level terms to avoid disclosing operationally sensitive information that would potentially serve to provoke attackers.

> *Given current malicious activities on the Internet, Netnod believes this requirement to be outdated. Making this data public would not benefit the overall service availability for the root service. Netnod remains committed to sharing this information with entities who can demonstrate a legitimate need for the information. Typical efforts in this category would be review and auditing activities initiated by the IANA functions operator, internal root server operator coordination efforts, ICANN's Root Server System Advisory*

Committee work, and select academic research projects. Netnod retains the right to determine, on a case-by-case basis, who shall be allowed access to this information.

3.5 Operational Security

[E.3.5-A] Individual Root Server Operators will adopt or continue to follow best practices with regard to operational security in the operation of their infrastructure.

Netnod follows and will continue to follow industry-standard best operation practices with regard to the operational security of our infrastructure.

[E.3.5-B] Root Server Operators shall publish high-level business continuity plans with respect to their Root Server infrastructure.

This provides confirmation to the Internet community that disaster recovery plans exist and are regularly reviewed and exercised.

Netnod's business continuity plan for the DNS root service is presented in a separate document, found at this URL:

https://www.netnod.se/sites/default/files/2019-03/netnod-rssac-001-business-cont.pdf

3.6 Diversity of Implementation

[E.3.6-A] Each Root Server Operator shall publish documentation that describes key implementation choices (such as the type of DNS software used) to allow interested members of the Internet community to assess the diversity of implementation choices across the system as a whole.

Individual Root Server Operators make implementation decisions autonomously, but in a coordinated fashion. In particular, Root Server Operators collaborate to ensure that a diversity of software and related service-delivery platform choices exists across the Root Server system as a whole. The goal of this diversity is to ensure that the system as a whole is not unnecessarily dependent on a single implementation choice, which might otherwise lead to a failure of the whole system due to a serious defect in a common component.

Netnod commits to share this information with entities who can demonstrate a legitimate need for the information. Typical efforts in this category would be review and auditing activities initiated by the IANA functions operator, internal root server operator coordination efforts, ICANN's Root Server System Advisory Committee work, and select academic research projects. Netnod retains the right to determine, on a case-by-case basis, who shall be allowed access to this information.

3.7 Monitoring and Measurement

[E.3.7-A] Each Root Server Operator will adopt or continue to follow best current

practices with respect to operational monitoring of elements within their infrastructure.

The goal here lies in identifying failures in service elements and mitigating those failures in a timely fashion.

> *Netnod's monitoring systems measures thousands of relevant parameters. It covers zone versions, network reachability, various server parameters, and more, over our entire infrastructure. We actively follow and take part in relevant discussions in the industry and adopt and adapt to emerging best practices as appropriate. This includes using the RIPE Atlas system to investigate potential service issues. We also monitor the results from the continuous tests run by the RIPE NCC in the DNSMON project.*

[E.3.7-B] Each Root Server Operator will adopt or continue to perform measurements of query traffic received and shall publish statistics based on those measurements.

The Internet technical community is then able to gauge trends and other effects related to production Root Server traffic levels.

> *Netnod publishes query traffic statistics in compliance with RSSAC002. The data can be obtained at: https://www.netnod.se/rssac002-metrics/*

[E.3.8.1-A] Individual Root Server Operators will continue to maintain functional communication channels between each other in order to facilitate coordination and maintain functional working relationships between technical staff.

Emergency communications channels exist to facilitate information sharing between individual Root Server Operators in real time in the event that a crisis requires it.

> *Netnod is an active participant in the root server operators' community and is connected to all common emergency communication channels.*

[E.3.8.1-B] All communications channels are to be tested regularly.

> *Channels are tested regularly three times per year at the recurring RSO technical meetings.*

3.8.2 Public Communication

[E.3.8.2-A] Individual Root Server Operators shall publish administrative and operational contact information to allow users and other interested parties to escalate technical service concerns.

> *Netnod publishes all relevant contact information on its web pages, including http://i.root-servers.org/ and https://www.netnod.se/. Specifically, the Netnod NOC emergency contact details are available here: https://www.netnod.se/about-netnod/contact-netnod. The NOC responds to telephone requests 24x7 and can relay requests for contact to all staff members and functions at*

Netnod.

This information is also reachable through the common entry point to the root server operators, found at http://www.root-servers.org/, at the top, when clicking "Netnod", and at the bottom under the "I" tab.

[End of RSSAC001 response]