RSSAC001 Version 2
Service Expectations of Root Servers Operators

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
1 August 2023

Preface

This is an Advisory to the Internet Corporation for Assigned Names and Numbers (ICANN) Board of Directors and the Internet community more broadly from the ICANN Root Server System Advisory Committee (RSSAC). In this Advisory, the RSSAC defines a set of service expectations that RSOs must satisfy.

The RSSAC seeks to advise the ICANN community and Board on matters relating to the operation, administration, security and integrity of the Internet's Root Server System. This includes communicating on matters relating to the operation of the Root Servers and their multiple instances with the technical and ICANN community, gathering and articulating requirements to offer to those engaged in technical revisions of the protocols and best common practices related to the operational of DNS servers, engaging in ongoing threat assessment and risk analysis of the Root Server System and recommend any necessary audit activity to assess the current status of root servers and root zone. The RSSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Advisory, references to RSSAC Caucus members' statement of interest, and RSSAC members' objections to the findings or recommendations in this Report are at the end of this document.

RSSAC001v2 was approved by the RSSAC on 08/01/2023.

Table of Contents

1. Introduction

Domain Name System (DNS) infrastructure includes elements known as Root Name Servers ("Root Servers"). This document defines the service expectations that Root Servers and root server operators (RSOs) are expected to meet as they provide root name service to the Internet community.

This document recognizes earlier guidance in the implementation and operation of Root Servers (RFC 2010,[1] 2870,[2] 7720[3]), and the part such guidance has played in the development of the DNS as a whole. Earlier guidance provided detailed requirements on the technical implementation of root name servers that was useful at the time it was written. However, technical approaches for deploying authoritative-only DNS servers have advanced since that time, and there is a useful diversity of implementation evident in the root server system as a whole today that would not be possible if the strict advice in earlier documents were to be followed precisely.

This document highlights that a diversity of approach is desirable in the root server system, and replaces earlier direction on implementation with a set of service expectations that RSOs must satisfy.

IETF Best Current Practice (BCP) 40[4] defines the protocol requirements and some deployment requirements for the Root Name Service.

In the remainder of this document each expectation is designated with an alphanumeric identifier (e.g., E.3.1-A) followed by a succinct description of the expectation itself in bold type. Paragraphs following each expectation provides further descriptive text and possible ways the expectation may be satisfied.

2. Service Provided by Root Servers

At the time of writing there are thirteen root server identifiers, operated by twelve different RSOs. An RSO is an organization responsible for managing the root service on IP addresses specified as entries in DNS root sources described in RSSAC030.[5] . A "root server identifier" is a DNS name associated with IP addresses in the root zone and the root hints file. These names are currently A.ROOT-SERVERS.NET through M.ROOT-SERVERS.NET (and are often referred to by letter, e.g., "M-Root"). A "root

[1] See RFC 2010: Operational Criteria for Root Name Servers, https://datatracker.ietf.org/doc/rfc2010/
[2] See RFC 2870: Root Name Server Operational Requirements, https://datatracker.ietf.org/doc/rfc2870/
[3] See RFC 7720: DNS Root Name Service Protocol and Deployment Requirements, https://datatracker.ietf.org/doc/rfc7720/
[4] See https://www.rfc-editor.org/info/bcp40
[5] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources, https://www.icann.org/en/system/files/files/rssac-030-04nov17-en.pdf

server" is the infrastructure maintained by a root server operator to provide the authoritative DNS root zone service at the IP addresses associated with a root server identifier. The infrastructure used to run a root server is distributed across numerous geographic sites. A root server "instance", or an "anycast instance", is the portion of a root server's infrastructure that serves root data at one site.

From a protocol perspective, a root server is a DNS name server that provides authoritative-only DNS service for the root zone.[6] DNS name servers receive queries from clients using the DNS protocol and provide appropriate responses.[7] The clients of root servers are, for the most part, caching DNS resolvers that send requests to authoritative-only servers in response to queries they receive from stub resolvers.

Root servers also serve additional zones. All root servers are authoritative for the ROOT-SERVERS.NET zone.

The root zone of the DNS has been signed using DNS Security Extensions (DNSSEC) since July 2010. Root servers support the corresponding DNS protocol extensions when sending responses.[8]

Each root server listens for queries on a set of IP addresses that are globally unique, and that are dedicated for use by that root server identifier, as described in RSSAC030.[9] Root servers occasionally change their IP addresses, although such events are not frequent. For example, an IPv6 address was added to D.ROOT-SERVERS.NET on 2011-06-10, and to I.ROOT-SERVERS.NET on 2010-06-17. F.ROOT-SERVERS.NET's IPv6 address was renumbered on 2008-01-22. Changes in service addresses for root servers are coordinated by the Internet Assigned Numbers Authority (IANA) Function[10] as part of the normal root zone management process.[11]

3. Expectations of Root Server Operators

This document describes the expectations placed upon RSOs as part of the service they provide. An RSO should make all reasonable efforts to satisfy these expectations. When unable to satisfy a particular expectation, the RSO should document the reason.

---

[6] See RFC 1034: Domain Names - Concepts and Facilities, https://datatracker.ietf.org/doc/rfc1034/
[7] See RFC 1035: Domain Names - Implementation and Specification, https://datatracker.ietf.org/doc/rfc1035/
[8] See RFC 9364: DNS Security Extensions (DNSSEC), https://datatracker.ietf.org/doc/rfc9364/
[9] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources: https://www.icann.org/en/system/files/files/rssac-030-04nov17-en.pdf.
[10] See https://www.iana.org/
[11] Internet Assigned Numbers Authority, http://www.iana.org/

3.1 Infrastructure

[E.3.1-A] Each RSO is expected 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 RSO.

A summary of the types of information RSOs are expected to publish can be found in Section 4 of this document.

[E.3.1-B] The RSOs are collectively expected to deliver the service in conformance to IETF standards and requirements as described in BCP 40.

BCP 40 describes the protocol and deployment requirements for the DNS root name service. The RSOs are expected to work together to provide the service in compliance with the requirements outlined in BCP 40.

[E.3.1-C] Each RSO is expected to notify the Internet community of service-impacting operational changes.

Changes such as adding or removing IPv4/IPv6 addresses have an impact on DNS implementations and systems such as DNS resolvers. RSOs are expected to announce changes that affect the RSO's service with sufficient advance notice. The amount of advance notice should be appropriate for the expected impact on deployed systems.

3.2 Service Accuracy

[E.3.2-A] Each RSO is expected to implement the current DNS protocol through appropriate software and infrastructure choices.

An RSO is expected to choose hardware, software, and other components that allow it to meet the protocol and deployment requirements specified in BCP 40.

[E.3.2-B] Each RSO is expected to accurately serve the IANA root zone.

This expectation is tied to principle #2 from RSSAC055, which states: "IANA is the source of DNS root data. RSOs are committed to serving the IANA global root DNS namespace. Root servers provide DNS answers containing *complete* and *unmodified* DNS data, including DNS Security Extensions (DNSSEC) data." Each RSO is expected to

always accurately serve the root zone provided by IANA via the Root Zone Maintainer (RZM).

[E.3.2-C] Each RSO is expected to serve up-to-date zone data.

An RSO is expected to make best/reasonable efforts to obtain and serve the latest version of the root zone as published by the RZM. No artificial or unnecessary delays should be added to the propagation of new zone versions throughout the RSO's infrastructure.

[E.3.2-D] Each RSO is expected to validate root zone data distributed by the RZM.

An RSO is expected to validate root zone data provided by the RZM to assure its integrity and authenticity. At a minimum, this means use of Transaction Authentication for DNS (TSIG) on zone transfers, which has been a requirement for transfering zone data from the RZM since March 2002.

An RSO is expected to document any additional root zone validity checks they utilize or implement, as well as how validity check failures are handled (e.g., serving most recently valid data, notifying the RZM, etc).

3.3 Service Availability

[E.3.3-A] Each RSO is expected to deploy their systems such that planned maintenance on individual infrastructure elements is possible without making the entire service of the RSO unavailable.

There should not be any planned maintenance associated with the operation of any root server that would make the corresponding service generally unavailable to the Internet.

3.4 Service Capacity

[E.3.4-A] Each RSO is expected to make all reasonable efforts to ensure that sufficient capacity exists in their deployed infrastructure to allow for substantial fluctuations in traffic loads.

Some events (such as software bugs, flash crowds, denial of service or other attacks) might present a significantly greater traffic 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. As stated in the FAQ published by the RSOs: "Root servers may limit or prevent responses to queries used in attacks or that otherwise cause a degradation of service to others. This is done only to protect the root service itself or to protect third parties targeted in reflection attacks."[12]

[12] See Root Server System Frequently Asked Questions, https://root-servers.org/faq/

3.5 Operational Security

[E.3.5-A] Each RSO is expected to follow best practices with regard to operational security in the operation of their infrastructure.

RSOs are expected to adhere to industry standard security practices. RFC 4778[13] ("Current Operational Security Practices in Internet Service Provider Environments") is an example of such published practices.

[E.3.5-B] Each RSO is expected to maintain business continuity plans with respect to its infrastructure.

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

3.6 Diversity of Implementation

[E.3.6-A] Each RSO is expected to share, possibly under non-disclosure agreement, details that describe key implementation choices with the other RSOs. The RSOs are expected to collectively publish aggregated implementation diversity reports from time-to-time.

Individual RSOs make implementation decisions autonomously, but in a coordinated fashion. In particular, RSOs collaborate to ensure that a diversity of software and related service-delivery platform choices exist across the RSS 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.

There are many different ways that an RSO might implement their diversity of choices, for example:

- Operating systems
- Name server software
- Routing software
- Virtualization software
- Server, routing, and switching hardware
- Use of third-party providers
- Network connectivity
- IP address resources
- Geography
- Skillsets of personnel

[13] See RFC4778 : Current Operational Security Practices in Internet Service Provider Environments, https://www.rfc-editor.org/rfc/rfc4778

The RSOs are expected to collectively publish aggregated implementation diversity reports from time-to-time. These reports serve to assure the community that the RSOs take implementation diversity seriously and provide a collective view of implementation choices within the root server system, without associating particular choices to particular RSOs.

3.7 Monitoring and Measurement

[E.3.7-A] Each RSO is expected to monitor elements within its own infrastructure.

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

[E.3.7-B] Each RSO is expected to perform measurements and publish statistics as specified in RSSAC002.

Each RSO is expected to publish their own RSSAC002 data on a daily basis. For more information, please see RSSAC002: Advisory on Measurements of the Root Server System.[14] A web page <https://root-servers.org/rssac002/> provides links to each RSO's RSSAC002 data location.

The Internet technical community is able to use this data to gauge trends and other effects related to production root server traffic levels.

3.8 Communication

3.8.1 Communication Between RSOs

[E.3.8.1-A] Each RSO is expected to maintain functional communication channels with the other RSOs in order to facilitate coordination and maintain functional working relationships between technical staff.

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

[E.3.8.1-B] Each RSO is expected to regularly exercise all communications channels.

To satisfy this expectation, an RSO should publicly confirm their participation in regular tests of RSO group communication channels.

3.8.2 Public Communication

[14] See RSSAC02v5: Advisory on Measurements of the Root Server System, available at <TBD>

Service Expectations of Root Server Operators

[E.3.8.2-A] Each RSO is expected to publish administrative and operational contact information.

The ability to reach RSO staff allows users and other interested parties to escalate technical service concerns.

4. Public Documentation

This document places expectations on individual root server operators to publish the following:

- Operationally relevant details of infrastructure, including service-delivery locations, addressing information and routing information.
- Statistics based on query traffic received.
- Operational contact information of each RSO to allow escalation of technical service concerns.

Each RSO publishes its own RSSAC001 statements at a location they control. A web page <https://root-servers.org/rssac001/> provides links to each RSO's published RSSAC001 documentation.

In addition, root server operators collectively are expected to publish aggregated implementation diversity reports as described in Section 3.6.

5. Recommendation

Recommendation 1: The RSSAC recommends each RSO publish one or more statements indicating their compliance with the expectations provided in this document.

6. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the RSSAC process. The Acknowledgments section lists the RSSAC caucus members, outside experts, and ICANN staff who contributed directly to this particular document. The Statement of Interest section points to the biographies of all RSSAC caucus members. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who

have recused themselves from discussion of the topic with which this Advisory is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of the RSSAC.

6.1 Acknowledgments

RSSAC thanks the following members of the Caucus and external experts for their time, contributions, and review in producing this Report.

RSSAC caucus members
John Augenstein
Frederick Baker
Marc Blanchet
Brett Carr
Kazunori Fujiwara
Wes Hardaker
Paul Hoffman
Hiro Hotta
Lars-Johan Liman
Jeff Osborn
Kenneth Renard
Karl Reuss
Shinta Sato
Barbara G. Schleckser
Ryan Stephenson
Robert Story
Brad Verd
Duane Wessels
Dessalegn Yehuala

ICANN support staff
Andrew McConachie
Ozan Sahin
Steve Sheng (editor)

6.2 Statements of Interest

RSSAC caucus member biographical information and Statements of Interests are available at:
https://community.icann.org/display/RSI/RSSAC+Caucus+Statements+of+Interest.

6.3 Dissents

There were no dissents.

6.4 Withdrawals

There were no withdrawals.

7. Revision History

7.1 Version 1

The first version of RSSAC001 was published on 4 December 2015, and is available at:https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf

7.2 Version 2

The second version of RSSAC001 was published on 1 August 2023, and is available at: TBD.

Changes include:

- Throughout - a number of grammatical and editorial changes.
- Throughout - apply RSSAC026 lexicon to the document.
- Throughout - changed endnote to footnote.
- Section 3.1 - added Expectation E3.1-C
- Section 3.3 - consolidate all expectations into one.
- Section 3.4 - removed E.3.4.-B.
- Section 3.6 - added explanatory text on E.3.6-A.
- Section 5 - removed recommendation 2.
- Appendix A - updated to match the latest list of expectations.

Appendix A: Summary of Expectations

[E.3.1-A] Each RSO is expected to publish operationally relevant details of their infrastructure, including service-delivery locations, addressing information and routing (e.g., origin autonomous system) information.

[E.3.1-B] The RSOs are collectively expected to deliver the service in conformance to IETF standards and requirements as described in BCP 40.

[E.3.1-C] Each RSO is expected to notify the Internet community of service-impacting operational changes.

[E.3.2-A] Each RSO is expected to implement the current DNS protocol through appropriate software and infrastructure choices.

[E.3.2-B] Each RSO is expected to accurately serve the IANA root zone.

[E.3.2-C] Each RSO is expected to serve up-to-date zone data.

[E.3.2-D] Each RSO is expected to validate root zone data distributed by the RZM.

[E.3.3-A] Each RSO is expected to deploy their systems such that planned maintenance on individual infrastructure elements is possible without making the entire service unavailable.

[E.3.4-A] Each RSO is expected to 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.

[E.3.5-A] Each RSO is expected to follow best practices with regard to operational security in the operation of their infrastructure.

[E.3.5-B] Each RSO is expected to maintain business continuity plans with respect to its infrastructure.

[E.3.6-A] Each RSO is expected to share, possibly under non-disclosure agreement, details that describe key implementation choices with the other RSOs. The RSOs are expected to collectively publish aggregated implementation diversity reports from time-to-time.

[E.3.7-A] Each RSO is expected to monitor elements within its own infrastructure.

[E.3.7-B] Each RSO is expected to perform measurements and publish statistics as specified in RSSAC002.

Service Expectations of Root Server Operators

[E.3.8.1-A] Each RSO is expected to maintain functional communication channels with the other RSOs in order to facilitate coordination and maintain functional working relationships between technical staff.

[E.3.8.1-B] Each RSO is expected to regularly exercise all communications channels.

[E.3.8.2-A] Each RSO is expected to publish administrative and operational contact information.