

Service Expectations of Root Servers Operators

RSSAC001 Version 22

Service Expectations of Root Servers Operators

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
4DD DecemberMonth 2015YY

Service Expectations of Root Servers Operators

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 ~~root server operator~~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 ~~11/20/2014~~MM/DD/YYYY. It was held for publication in tandem with ~~a RFC~~an update to BCP 40 by the IAB, specifying the DNS Root Name Service Protocol and Deployment Requirements. In ~~December 2015~~MM YYYY, the IAB RFC was published as RFC ~~7720~~ [7720-bis].

Service Expectations of Root Servers Operators

Table of Contents

1. Introduction	4
2. Service Provided by Root Servers	4
3. Expectations of Root Server Operators	5
3.1 Infrastructure	5
3.2 Service Accuracy	5
3.3 Service Availability	6
3.4 Service Capability	7
3.5 Operational Security	7
3.6 Diversity of Implementation	8
3.7 Monitoring and Measurement	8
3.8 Communication	8
3.8.1 Inter-Operator Communication	8
3.8.2 Public Communication	9
4. Public Documentation	9
5. Recommendation	9
6. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals	9
6.1 Acknowledgments	10
6.2 Statements of Interest	10
6.3 Dissents	10
6.4 Withdrawals	10
7. Bibliography	11
Appendix A: Summary of Expectations	12
1. Introduction	4
2. Service Provided by Root Servers	4
3. Expectations of Root Server Operators	5
3.1 Infrastructure	5
3.2 Service Accuracy	6
3.3 Service Availability	7
3.4 Service Capacity	7
3.5 Operational Security	7
3.6 Diversity of Implementation	8
3.7 Monitoring and Measurement	8

Service Expectations of Root Servers Operators

3.8 Communication	9
3.8.1 Communication Between RSOs	9
3.8.2 Public Communication	9
4. Public Documentation	9
5. Recommendation	10
6. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals	10
6.1 Acknowledgments	10
6.2 Statements of Interest	11
6.3 Dissents	11
6.4 Withdrawals	11
7. Revision History	11
7.1 Version 1	11
7.2 Version 2	11
Appendix A: Summary of Expectations	13

Service Expectations of Root Servers Operators

1. Introduction

Domain Name System (DNS) infrastructure includes elements known as Root Name Servers (“Root Servers”). – This document ~~describes the best practice service provided by Root Servers, and defines the expectations that users might reasonably hold of both that service and the Root Server Operators.~~ 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 7720³) ~~[5][6]~~, 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 ~~root server operator~~RSOs must satisfy.

IETF Best Current Practice (~~RFC2870 is updated by RFC 7720 [4]BCP~~) 40⁴, ~~which~~ 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 Servers~~root server identifiers, operated by twelve different ~~RSO~~organizations. ~~Root Servers are named A.ROOT-SERVERS.NET through M.ROOT-SERVERS.NET, and are often referred to by letter (e.g. “L-Root”).~~ ¶

~~¶ Although the word “server” is still used to identify the infrastructure providing service for individual letters, service is generally provided using techniques that involve more~~

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/rfc2870/>

⁴ <https://www.rfc-editor.org/info/bcp40>

Service Expectations of Root Servers Operators

~~elaborate infrastructure than is suggested by that word. For example, many Root Servers provide service using multiple individual name server elements using anycast [1], rather than being provided by a single server. In this document, "Root Server" refers generally to the service provided by the infrastructure operated by a Root Server Operator, and not to individual infrastructure elements. 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 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~~root server is a DNS name server that provides authoritative-only DNS service for the root zone ~~[7]~~.⁶ – ~~Such~~DNS name servers receive queries from clients using the DNS protocol ~~[8]~~ and provide appropriate responses.⁷ ~~€~~The clients of ~~Root Servers~~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 ~~S~~servers also serve additional zones. –All ~~Root Servers~~root servers are authoritative for the ROOT-SERVERS.NET zone ~~and currently twelve of the thirteen are authoritative for the ARPA zone⁸.~~

The root zone of the DNS was signed using DNS Security Extensions (DNSSEC) ~~[2]~~ in July 2010. –Root ~~S~~servers support the corresponding DNS protocol extensions ~~[3]~~ when sending responses.⁹

Each ~~R~~root ~~S~~server listens for queries on a set of IP addresses that are globally unique, and that are dedicated for use by that ~~R~~root ~~S~~server identifier. –~~At the time of writing~~ ~~ll~~some ~~R~~root ~~S~~servers ~~listen on a single IPv4 address, and some~~ listen on both a single IPv4 address and a single IPv6 address. – Root ~~S~~servers ~~are renumbered~~ occasionally ~~change their IP addresses~~, although such events are not frequent.¹⁰ For example, an IPv6 address was added to D-Root on 2011-06-10, and to I-Root on 2010-06-17. F-Root's IPv6 address was renumbered on 2008-01-22. Changes in service addresses for ~~R~~root ~~S~~servers

⁵ See RSSAC030: RSSAC Statement on Entries in DNS Root Sources, <https://www.icann.org/en/system/files/files/rssac-030-04nov17-en.pdf>

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 ~~All root servers apart from J-Root currently serve the ARPA zone.~~

⁹ See RFC 9364: DNS Security Extensions (DNSSEC), <https://datatracker.ietf.org/doc/rfc9364/>

¹⁰ ~~For example, an IPv6 addresses was added to D-Root on 2011-06-10, and to I-Root on 2010-06-17. F-Root's IPv6 address was renumbered on 2008-01-22. A summary of historical addressing changes can be found at <http://www.root-servers.org/>~~

Service Expectations of Root Servers Operators

are coordinated by the IANA Function[#] as part of the normal ~~R~~root ~~Z~~zone ~~M~~management process.¹² A summary of historical addressing changes can be found at <http://www.root-servers.org/>.

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.

3.1 Infrastructure

~~[E.3.1-A] Individual Each Root Server Operator~~ RSOs ~~are~~ ~~is~~ expected 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 ~~R~~root ~~S~~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~~ RSO.

A summary of all information published by RSOs can be found in Section 4 of this document.

~~[E.3.1-B] Individual Each Root Servers~~ RSO ~~will~~ is expected to 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~~ BCP 40.

~~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.

~~[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~~

~~[#] Internet Assigned Numbers Authority, <http://www.iana.org/>~~

~~¹² Internet Assigned Numbers Authority, <http://www.iana.org/>~~

~~[#] A summary of all information published by root server operators, as described in this document, can be found in a later section.~~

Service Expectations of Root Servers Operators

currently resigned every time it is published, so the DNSSEC signatures (i.e., RRSIG records) change with each new zone.

~~[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.

~~[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.~~

BCP 40 describes the protocol and deployment requirements for the DNS root name service. An RSO is expected 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.

Service Expectations of Root Servers Operators

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 always 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 transferring 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] Individual Root Servers are to be deployed such that planned maintenance on individual infrastructure elements is possible without any measurable loss of 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 unavailable.

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

Service Expectations of Root Servers Operators

~~[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 ~~R~~root ~~S~~ervers. – The DNS protocol accommodates unavailability of individual ~~Root Servers~~RSIs without significant disruption to the DNS service experienced by end users. However, each ~~root server operator~~RSO shall employ best efforts in engineering and assign appropriate resources that ensures a commensurate level of component redundancy for ~~the each Root Server they operate~~RSI. ¶

~~[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. ¶~~

¶

3.4 Service ~~Capability~~Capacity

~~[E.3.4-A] Individual Each Root Server Operators~~RSO ~~will~~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.

¶

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. ~~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.” Filtering techniques may be employed by Root Server Operators to maintain service to legitimate DNS queries.~~

¶

~~[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.¹⁴~~

¹⁴ See Root Server System Frequently Asked Questions, <https://root-servers.org/faq/>
RSSAC001-v2

Service Expectations of Root Servers Operators

3.5 Operational Security

[E.3.5-A] ~~Individual~~ Each Root Server Operator RSO ~~will~~ is expected to ~~adopt or continue 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 (“Current Operational Security Practices in Internet Service Provider Environments”) is an example of such published practices.

[E.3.5-B] Each Root Server Operator RSO ~~shall~~ is expected to ~~publish high-level maintain~~ business continuity plans with respect to ~~their~~ its Root Server 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 Root Server Operator RSO ~~shall~~ is expected to 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~~ RSS as a whole.

Individual Root Server Operator RSOs make implementation decisions autonomously, but in a coordinated fashion. – In particular, Root Server Operator RSOs collaborate to ensure that a diversity of software and related service-delivery platform choices exists across the Root Server system 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, including:

- 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

Service Expectations of Root Servers Operators

3.7 Monitoring and Measurement

~~[E.3.7-A] Each Root Server Operator RSO willis expected to adopt or continue to follow best current practices with respect to operational monitoring of elements within their infrastructure. monitor elements within its own infrastructure.~~

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

~~[E.3.7-B] Each Root Server Operator RSO willis expected to adopt or continue to perform measurements of query traffic received and shall publish statistics based on those measurements. ¶~~
and publish statistics as specified in RSSAC002.

~~The Internet technical community is then able to gauge trends and other effects related to production Root Server traffic levels.¹⁶ 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.¹⁶ 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 ~~Inter-Operator~~ Communication Between RSOs

~~[E.3.8.1-A] IndividualEach Root Server Operators RSO willis expected continue to maintain functional communication channels between eachwith 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 ~~Root Server Operator~~ RSOs in real time in the event that a crisis requires it.

~~[E.3.8.1-B] AEach RSO is expected to regularly exercise all communications channels ~~are to be tested regularly.~~~~

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

¹⁵ For more information, please see RSSAC002: Advisory on Measurements of the Root Server System. Available at <<https://www.icann.org/resources/pages/rssac-publications-2014-05-12-en>>

¹⁶ See RSSAC02v5: Advisory on Measurements of the Root Server System, available at <TBD>
RSSAC001-v2

Service Expectations of Root Servers Operators

3.8.2 Public Communication

[E.3.8.2-A] ~~Individual~~ Each Root Server Operator RSO shall be expected to publish administrative and operational contact information ~~to allow users and other interested parties to escalate technical service concerns.~~

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

4. Public Documentation

This document specifies ~~that~~ many aspects of the operation of individual ~~R~~root ~~S~~servers that are expected to be published:

- Operationally relevant details of infrastructure, including service-delivery locations, addressing information and routing information.
- ~~A commitment to service availability through maintenance scheduling and notification of relevant operational events.~~
- ~~Infrastructure capacity, including details of current steady state load and maximum estimated capacity available.~~
- ~~High level business continuity plans.~~¶
- Key implementation choices, such as the type ~~of DNS software deployed~~ of hardware and software in use.
- Statistics based on query traffic received.
- Operational contact information ~~of each RSO~~ to allow escalation of technical service concerns.

¶

All documentation is published at <http://www.root-servers.org/> or, if published elsewhere, is linked to from that page.

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

5. Recommendation

~~Recommendation 1: The RSSAC recommends each root server operator publish the level of service they offer as a root server operator to the Internet Community by responding to each of the expectations detailed herein.~~

¶

Service Expectations of Root Servers Operators

~~Recommendation 2: The RSSAC recommends that each root server operator advise the RSSAC as to where this RSSAC001 responses have been published, and notify RSSAC of future revisions or either content or location.~~

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

~~TBD~~

John Augenstein

Frederick Baker

Brett Carr

Kazunori Fujiwara

Wes Hardaker

Paul Hoffman

Hiro Hotta

Jeff Osborn

Kenneth Renard

Karl Reuss

Shinta Sato

Barbara G. Schleckser

Ryan Stephenson

Robert Story

Service Expectations of Root Servers Operators

Brad Verd
Duane Wessels
Dessalegn Yehuala

ICANN support staff

TBD
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. BibliographyRevision 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 DD MM 20YY, 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.

Service Expectations of Root Servers Operators

- 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.

- [1] ~~Abley, J., & Lindqvist, K. (2006). BCP 126, RFC 4786. Operation of Anycast Services.~~
- [2] ~~Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). RFC 4033. DNS Security Introduction and Requirements.~~
- [3] ~~Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). RFC 4035. Protocol Modifications for the DNS Security Extensions.~~
- [4] ~~Blanchet, M., Liman, L-J., 2015. RFC7720. DNS Root Name Service Protocol and Deployment Requirements.~~
- [5] ~~Bush, R., Karrenberg, D., Koster, M., & Plzak, R. (2000). RFC 2870. Root Name Server Operational Requirements.~~
- [6] ~~Manning, B., & Vixie, P. (1996). RFC 2010. Operational Criteria for Root Name Servers.~~
- [7] ~~Moekapetris, P. (1987). STD 13, RFC 1034. Domain names - concepts and facilities.~~

~~Moekapetris, P. (1987). STD 13, RFC 1035. Domain names - implementation and specification.~~

Service Expectations of Root Servers Operators

Appendix A: Summary of Expectations

~~{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.¶~~

~~¶~~

~~{E.3.1-B} Individual Root Servers will deliver the service in conformance to IETF standards and requirements as described in RFC7720 and any other IETF standards defined Internet Protocol as deemed appropriate¶~~

~~¶~~

~~{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.¶~~

~~¶~~

~~{E.3.2-B} Individual Root Servers will serve accurate and current revisions of the root zone.¶~~

~~¶~~

~~{E.3.2-C} Individual Root Servers will continue to provide “loosely coherent” service across their infrastructure.¶~~

~~¶~~

~~{E.3.2-D} All Root Servers will continue to serve precise, accurate zones as distributed from the Root Zone Maintainer.¶~~

~~¶~~

~~{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.¶~~

~~¶~~

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

~~¶~~

~~{E.3.3-C} Each root server operator shall publish documentation that describes the operator’s commitment to service availability through maintenance scheduling and notification of relevant operational events.¶~~

~~¶~~

~~{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.¶~~

~~¶~~

~~{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.¶~~

~~¶~~

~~{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.¶~~

Service Expectations of Root Servers Operators

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

~~¶
[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.¶~~

~~¶
[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.¶~~

~~¶
[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.¶~~

~~¶
[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.¶~~

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

~~¶
[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.~~

[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] Each RSO is 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.

Service Expectations of Root Servers Operators

[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 publish documentation that describes key implementation choices to allow interested members of the Internet community to assess the diversity of implementation choices across the RSS as a whole.

[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.

[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.