

RIPE NCC Statement on RSSAC001v2 "Service Expectations of Root Servers Operators"

Author: RIPE NCC

Document ID: ripe-859

Date: 8 May 2026

Background

ICANN's Root Server System Advisory Committee (RSSAC) published [RSSAC001v2](#) which describes various expectations that root server operators should satisfy. The document lists one recommendation:

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

This is the RIPE NCC's response to this recommendation as operator of k.root-servers.net.

Below are statements corresponding to each of the service expectations for Root Server operators outlined in RSSAC001v2.

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 RIPE NCC publishes operationally relevant infrastructure details at these locations:

<https://k.root-servers.org>

<https://rest.db.ripe.net/ripe/aut-num/AS25152.txt>

<https://as25152.peeringdb.com>

[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](#).

The RIPE NCC delivers root DNS service in conformance with IETF standards and requirements described in BCP 40.

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

The RIPE NCC notifies the Internet community of service-impacting operational changes by posting messages to the RIPE DNS Working Group mailing list, DNS-OARC's DNS



Operations mailing list, the North American Network Operators Group (NANOG) mailing list and publishes a service update on the status page: <https://status.ripe.net/>.

Service Accuracy

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

The RIPE NCC delivers the root DNS service conforming to IETF standards and requirements described in BCP 40.

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

The RIPE NCC serves the IANA root zone and responds with complete and unmodified data on k.root-servers.net infrastructure.

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

The RIPE NCC monitors that k.root-servers.net serves up-to-date zone data.

Due to a large number of anycast sites there may occasionally be brief periods where zone data differ slightly between sites or servers as updates propagate.

In case a site becomes isolated from our controlling infrastructure, the site will autonomously continue serving the root zone. Service will automatically be withdrawn after the zone expires. This is in accordance with the SOA record's expire field as provided by IANA.

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

The RIPE NCC uses DNS Transaction SIGNatures (TSIG) to validate and protect the zone data while in transit from the Root Zone Maintainer and from our own distribution systems to the globally distributed anycast sites.

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.

The RIPE NCC performs maintenance on its systems by taking individual sites or components out of service. Due to built-in redundancies this does not affect the service of k.root-servers.net as a whole.

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 flash crowds or denial of service (DoS) attacks.



The RIPE NCC's systems are provisioned with sufficient capacity.

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.

Our approach to organisational security focuses on people, processes, and technology. This includes employee screening, security awareness training, access and asset management, a clear code of conduct and structured incident response procedures - all integrated to protect our information and maintain compliance across the organisation.

Our infrastructure security measures protect our network and systems from unauthorised access, data breaches, and operational disruptions. Through techniques like network segmentation, vulnerability management, encrypted remote access, proactive monitoring, and regular backups, we maintain a secure and resilient technology environment.

For more details visit the RIPE NCC Trust Portal: <https://trust.ripe.net/>.

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

The RIPE NCC has a business continuity plan in place for k.root-servers.net. This plan is regularly reviewed and exercised.

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.

The RIPE NCC operates at least two, but usually three, diverse code bases for DNS services from different open source vendors. The RIPE NCC operates two diverse code bases for software BGP routers from different open source vendors and two diverse hardware router implementations.

Additional technical details are regularly made available to the other root server operators in the interest of ensuring technical and operational diversity among RSOs.

Monitoring and Measurement

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



The RIPE NCC employs extensive 24x7 monitoring and alerting, including distributed monitoring from over ten thousand vantage points using [RIPE Atlas](#).

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

The RIPE NCC publishes RSSAC002 statistics at:
<https://www-static.ripe.net/dynamic/rssac002-metrics/>

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.

The RIPE NCC participates in the regular root server operators meetings and the various agreed methods of communications with other RSOs.

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

Communication channels are either exercised by daily use or through regular testing during root server operator meetings.

Public Communication

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

Contact information for k.root-servers.net can be found at:
<https://k.root-servers.org>
<https://rest.db.ripe.net/ripe/aut-num/AS25152.txt>
<https://as25152.peeringdb.com/>

The RIPE NCC can be contacted at: <https://ripe.net/contact/>.