Verisign Statement on RSSAC001v2 Service Expectations of Root Servers

Background

RSSAC001v2 is a publication of ICANN's Root Server System Advisory Committee that describes various service-related expectations on root server operators. This is Verisign's response to 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.

Verisign publishes operationally relevant infrastructure details through the root-servers.org web site. To view this information, scroll to the bottom of https://www.root-servers.org and select "A" under the Root Servers heading.

[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.

Verisign delivers root DNS service in conformance with the IETF standards and requirements as described in BCP 40.[1]

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

For operational changes that have the potential to impact end users, Verisign provides notice to the Internet Community by posting messages to operator forums such as DNS-OARC's DNS Operations mailing list and the North American Network Operators Group (NANOG) mailing list.

Service Accuracy

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

[1] https://www.rfc-editor.org/info/bcp40 -- DNS Root Name Service Protocol and Deployment Requirements

Verisign delivers root DNS service in compliance with the protocol requirements described in BCP 40.

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

Verisign serves only the IANA root zone and responds with complete and unmodified data on its root server infrastructure.

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

Verisign ensures that its root server systems always serve up-to-date zone data and reinforces this expectation with active monitoring.

Due to the large number of anycast sites and backend servers, there may occasionally be brief periods during which zone data differs slightly between sites or servers as updates are propagated.

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

Verisign uses DNS Transaction Signatures (TSIG) to validate zone data received from the root zone distribution system.

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.

When Verisign performs maintenance on its systems, individual sites and components are taken out of service without making the service unavailable.

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.

Verisign's systems are provisioned such that sufficient capacity exists to allow for substantial flash crowds or DoS attacks. This includes network capacity, software, and hardware components. Verisign may use traffic engineering techniques to shift traffic away from particular sites when under attack.

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.

Verisign maintains best practices with regard to operational security. We follow the 'three lines of defense' model[2] in the risk management and control of our business resiliency program: functions that own and manage risk, functions that oversee risks, and functions that provide independent assurance.

Verisign incorporates numerous protection layers in a globally distributed infrastructure, to include zero trust principles, network and data segmentation, intrusion detection and prevention, secure system images, multifactor authentication, and more, all reporting back to our 24X7 NOC. Our continuous monitoring program employs a mix of external and internal assessments including red teaming, physical and cybersecurity program reviews and testing, application security testing, phishing exercises, bug bounty programs, regulatory audits, and security framework assessments.

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

Verisign has developed, implemented, and tested business continuity and IT disaster recovery plans to mitigate the effects of natural, man-made, or technological disasters. Our plans are regularly tested, validated, and updated so that Verisign systems, services and key business functions can be operational in the event of any incident or disaster. Detailed Business Continuity Plans and Technical Disaster Recovery Plans are in place to address the restoration of information systems services and key business functions.

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.

Verisign uses two diverse code bases for DNS root service: (1) our proprietary and patented ATLAS resolution platform, and (2) the open-source NLnet Labs Name Server Daemon (NSD) software. One, the other, or both implementations may be in use at any given time.

Verisign further utilizes diversity in its geographic locations, choice of data center and transit providers, operating system vendors, and more.

[2] https://www.theiia.org/en/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/

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 their own infrastructure.

Verisign employs extensive monitoring and alerting via its 24x7 Network Operations Center (NOC).

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

Verisign publishes RSSAC002 statistics for A-root at https://a.root-servers.org/rssac-metrics/raw/.

Communication

[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.

Verisign participates in the regular root server operators meetings and the various methods of communications enabled by the RSO shared collaboration system.

[E.3.8.1-B] RSOs are expected to regularly exercise all communications channels.

Verisign participates in all RSO communication channels. Some of these are naturally exercised on a daily or weekly basis. Others, such as the emergency alert system, are exercised through regular testing.

Public Communication

[E.3.8.2-A] Each RSO is expected to publish administrative and operational contact information to allow users and other interested parties to escalate technical service concerns.

Verisign publishes a contact address for questions or concerns related to its root DNS service on the root-servers.org web site. Look for the “Contact Email” button on the page.