RSSAC Statement on the Client Side Reliability of Root DNS Data

28 June 2016

The RSSAC confirms that the operators of the root servers[1] are committed to serving the IANA global root DNS namespace. All root servers operated by these operators provide DNS answers containing complete and unmodified DNS data. This data residing in the root zone originates from the IANA Functions Operator and is received using security enhanced protocols through the agreed upon publication channels. The same cryptographically verifiable data is provided worldwide from all instances of these root servers to allow clients to detect tampering and ensure the integrity of the data.

The RSSAC fully supports the IAB's viewpoints expressed in RFC 2826, summarized in this quote: “To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS.”

For this to be true, it is paramount that DNS data can be relied upon at all times and in all locations of the Internet. The operators of the root servers are committed to serving all clients equally.

DNSSEC provides the means for a DNS client to cryptographically validate that DNS data have not been altered. The root zone has been signed with DNSSEC since 2010, and this allows clients to validate that they are receiving authentic data.

The RSSAC believes that modifying or tampering with root server responses undermines the predictability of the Internet as a dependable means of communication. The RSSAC reiterates its support for integrity protecting protocols such as DNSSEC.

[1] https://www.iana.org/domains/root/servers