Response to ICANN Public Comment[1]
Draft Report of the Root Zone DNSSEC Algorithm Rollover Study

Cloudflare is a global operator of Internet-facing services, an accredited registrar and the operator of 1.1.1.1, a global, public open resolver service which performs DNSSEC validation. We have extensive experience in DNSSEC protocol design and operation and our authoritative DNS services are notable for their online DNSSEC signing capabilities using non-RSA algorithms.

We have reviewed the Root Zone Algorithm Rollover Study (Draft) dated 19 October 2023.[2] We think the report provides sensible advice and addresses the scope of what the design team was asked to consider. We think the report provides a solid foundation on which detailed, technical implementation plans can be developed, and we encourage ICANN and other stakeholders to proceed with that work without delay.

We notice that the report makes reference to concerns relating to larger DNS responses from root servers, and of truncated responses that might lead to increased use of TCP transport in queries and responses.

Many large consumers of root zone data do not normally send queries to root servers at all. Examples include Cloudflare's 1.1.1.1 service and systems that follow the guidance in RFC 8806. These systems will not contribute to and cannot be affected by any change in root server query/response behaviour. In these cases, impact on end users is independent of the availability of TCP transport. We think this is worth noting.

In our experience responses from resolvers to end users are usually satisfied with data about TLD servers that is cached locally. The Root Server System needs to be consulted quite infrequently, and hence is rarely in the hot path of preparing a response for an end-user, especially in resolvers that pre-fetch cached data that is nearing expiry. When a referral from the Root Server System *is* needed, there are thirteen different root servers, over 1,700 individual

1 https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023

2 https://itp.cdn.icann.org/en/files/domain-name-system-security-extensions-dnssec/draft-report-root-zone-dnssec-algorithm-rollover-study-19-10-2023-en.pdf

anycast instances, intentional diversity in operational characteristics and a query-response protocol that accommodates retries.

For these reasons and others, we think a reduction in the availability of TCP transport due to large responses is quite unlikely to cause a problem for end users, and we think this is reflected in the experience to date with changes in the Root Server System that have resulted in an increase in response sizes.

While we agree that caution is prudent and necessary, we think it is important that the potential risk be assessed objectively and is not overstated. The primary reason for such caution should be to avoid undesirable impact on end users.

We hope these remarks are of use to you, and we look forward to your future work in this area. If we can be of assistance in the future, please do not hesitate to let us know.

Cloudflare
27 November 2023