

2018 KSK Rollover Monitoring Plan

Revised from 2017 KSK Rollover Monitoring Plan

ICANN Office of the Chief Technical Officer
27 April 2018



Introduction

This document describes the plan to monitor the traffic towards root name servers to evaluate the effects of changing the root zone KSK. The results of this monitoring effort will help ICANN understand the scale of possible failures due to rolling the KSK. It updates the [2017 KSK Rollover Monitoring Plan](#).

During the rollover of KSK-2010 to KSK-2017, ICANN plans to capture and analyse traffic to the ICANN-Managed Root Server (*IMRS*, also known as *L-root*) in near real time to understand the scale of resolvers that have problems with the KSK rollover. To make sure that the sample is statistically representative, a comparison will be made with traffic to other root servers who share data with ICANN.

A subset of resolvers that send traffic to the IMRS currently perform validation using DNSSEC. Some of these resolvers are able to follow the KSK rollover by implementing the protocol described in RFC 5011. In other cases, the resolvers' operators will configure a new trust anchor manually. But some resolvers will not have the root trust anchor updated and validation will fail. It is important to first establish a baseline to understand the behavior before rolling the key. There might be anomalies during this time, but measuring before the roll makes sure that these anomalies are part of the baseline. The underlying premise is that validating resolvers that do not have the new KSK will behave differently than those that do.

Expected Anomalies

During the rollover process, the response size for a DNS query for the DNSKEY resource records for the root zone will change. At some point, there will be more than two keys in the root DNSKEY resource record set. This larger packet size might lead to incomplete fragments received by the resolver, fallback to TCP, or both. These effects are referred to as “response size effects”.

Resolvers that have a “stale” trust anchor (meaning a trust anchor that has not been updated for some reason during the rollover process) will not be able to validate the root zone once the new KSK begins signing the key set. This situation will also have an effect on root server traffic because these resolvers might increase their query rate. These are referred to as “stale key effects”.

Stale key effects are measured based on the volume of requests and the number of unique AS numbers that are associated with the source IP addresses of those requests. In this way, the scale of impact can be understood.

Measurement Infrastructure

To cope with the sheer volume of requests and to process these requests in a timely fashion, ICANN has deployed a new measuring infrastructure.

Traffic to IMRS is captured locally at Anycast instances. Compressed traffic captures are then moved to the storage location for further processing. This storage location is either ICANN's LAX or DC data center, depending on availability and bandwidth. Traffic for other root server operators is stored at the ICANN data centers as well.

The measuring infrastructure consists of two large machines, one for the DC location and one for the LAX location. Custom analysis software has been deployed and is already in daily use analysing IMRS traffic.