
# 2017 KSK Rollover External Test Plan

Version: 2016-07-22

# Contents

# Introduction

This document covers the preparation of operational test environments, accessed by the general Internet public, to evaluate whether external systems are prepared to participate in the KSK rollover.

## Public Test Environments

ICANN will provide two public test environments for testing: one providing multiple key rollovers in real time, and one providing continuous key rollovers using accelerated time.

The target audience for the *real time 5011 environment* is DNS resolver operators and is designed for validating deployed software configurations and can be used in production environments.

The *accelerated 5011 environment* is intended for software developers. Because this environment requires modified RFC 5011 timers as well as a special root zone, it should not be used in production environments.

## Real Time 5011 Environment

The *real time 5011 environment* allows operators of validating resolvers to test whether their systems are likely to work during the KSK rollover if they are using RFC 5011. It has been reported that some distributions of resolver software are misconfigured so that after the 30-day hold down is complete, the new KSK is not written to permanent storage. This testbed will allow operators to test their configuration before the new KSK is installed into the root. The tests will take place in test zones far down the DNS hierarchy, and will not affect any of the root zone trust anchors or the signatures on the root zone.

### Goals

This testbed allows resolver operators to test their production systems without having to reboot or to change their normal settings. The test determines (in order):

- **Can you accept a new KSK?**
- **Can you accept signatures using the new KSK after 30 days?**
- **Can the validator continue to validate with the new trust anchor after a restart or reboot?**
- **Can you handle revocation of the original key?**

## Test Configuration

The test environment consists of a number of test zones -- **YYYYMMDD.testing.kskroll.icann.org** -- each zone starting a full 5011 compliant key rollover on the date given in the zone name.

Each zone starts off signed by a common key. On the date given in the zone name, the new KSK is introduced. A single key pair is used for all the original KSKs, and a second key pair for all of the rolled-to KSKs in order to make checking easier. After 31 days, the zone is signed with the new key. After another 10 days, the old key is published in the zone with the revoked bit turned on.

Each zone has a TXT RRset that has a record describing the test and pointing to a URL. There is also a TXT record that has the current state of the zone.

At the time of publication, this test environment is still under development. When the environment is ready, there will be a web page at testing.kskroll.icann.org that describes this testbed and has links to all of the keys.

## Communications

People using the testbed are encouraged to sign up for updates by email based on the zone that they are testing. A message will be sent day 24 reminding participants of the test, another at day 31 saying that they should check their trust anchor store, and another at day 41 talking about the revocation. Finally, a message is sent around day 50 reminding people to maybe remove their trust anchors for this test.

# Accelerated 5011 Environment

The *accelerated 5011 test environment* allows software developers to test all phases of the root KSK rollover in an accelerated (compressed) timeframe. This is implemented

by running through the 27 time "slots" that constitute the planned KSK roll in 27 minutes. This is achieved by moving forward one slot per minute instead of the normal ten days per slot. Because this environment proceeds faster than real time, this test requires modified RFC 5011 timers in order to work.

The accelerated 5011 test environment also includes a signed Trust Anchor XML corresponding to the current keys, thus reflecting changes that will be visible on the IANA web site.

The test root zone is served by one nameserver with a single IPv4/IPv6 address pair. In order to mimic the production root zone, the test root zone lists 13 name servers, uses name server hostnames with the same length as the real root zone, and contains the same number of A/AAAA glue records. A single domain (test.) is delegated from the test root zone.

The environment provides introspection via a web interface, enabling testers to get information on what keys are currently use for signing and when the next state change will happen. Example configurations files for various resolver implementations are also provided.

 ICANN will provide an accelerated test environment based on the one provided at **www.toot-servers.net**.

# Resolver Implementation Testing

ICANN will build an automated test suite test for resolvers bundled with various popular operating systems/distributions. The tests are performed by launching virtual machines and/or containers, and executing tests with the real time and the accelerated 5011 environments. These tests will also be run in ICANN's middlebox test lab.

The results and the test suite source code will be published to the public. Any issues will be reported back to the developers via appropriate channels.

An approximate list of the operating systems/distributions that will be tested is:

**LINUX (RPM)**

- CentOS 6
- CentOS 7

- Fedora 23
- Fedora 24
- Fedora 25 (rawhide)
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise Server 11
- SUSE Linux Enterprise Server 12

**LINUX (DEB)**

- Debian 8 "jessie"
- Debian 9 "stretch" (unreleased)
- Raspbian 8 "jessie"
- Ubuntu 12.04
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 16.10 (unreleased)

**LINUX (other)**

- Arch Linux
- Gentoo Linux

**BSD**

- FreeBSD 9
- FreeBSD 10
- NetBSD 6
- NetBSD 7
- OpenBSD 5.8
- OpenBSD 5.9

# Software Vendor Testing

ICANN will work with DNS software vendors to facilitate testing using the public test environments. The following implementations have been identified:

## Open Source Implementations

- BIND
- Unbound
- DNSMASQ
- Knot Resolver
- PowerDNS Recursor
- systemd resolved

## Commercial Implementations

ICANN will work with DNS software vendors to facilitate testing using the public test environments. The following implementations have been identified:

- Infoblox (based on BIND)
- Bluecat (based on BIND)
- Secure64 DNS Cache (based on Unbound)
- Windows Server
- Nominum Vantio CacheServe


# One World, One Internet

ICANN.ORG