# The Root Canary: Monitoring and Measuring the DNSSEC Root Key Rollover

R. van Rijswijk-Deij
University of Twente, SURFnet
r.m.vanrijswijk@utwente.nl

T. Chung, D. Choffnes, A. Mislove
Northeastern University

W. Toorop
NLnet Labs

## ABSTRACT

The Domain Name System (DNS) is part of the core of the Internet. Over the past decade, much-needed security features were added to this protocol, with the introduction of the DNS Security Extensions. DNSSEC adds authenticity and integrity to the protocol using digital signatures, and turns the DNS into a public key infrastructure (PKI). At the top of this PKI is a single key, the so-called Key Signing Key (KSK) for the DNS root. The current Root KSK was introduced in 2010, and has not changed since. This year, the Root KSK will be replaced for the first time ever. This event potentially has a major impact on the Internet. Thousands of DNS resolvers worldwide rely on this key to validate DNSSEC signatures, and must start using the new key, either through an automated process, or manual intervention. Failure to pick up the new key will result in resolvers becoming completely unavailable to end users. This work presents the "Root Canary", a system to monitor and measure this event from the perspective of validating DNS resolvers for its entire nine-month duration. The system combines three active measurement platforms to have the broadest possible coverage of validating resolvers. Results will be presented in near real-time, to allow the global DNS community to act if problems arise. Furthermore, after the Root KSK rollover concludes in March 2018, we will use the recorded datasets for an in-depth analysis, from which the Internet community can draw lessons for future key rollovers.

## CCS CONCEPTS

• **Networks → Naming and addressing**;

## KEYWORDS

DNS; DNSSEC; active measurements; Internet stability

**ACM Reference Format:**
R. van Rijswijk-Deij, T. Chung, D. Choffnes, A. Mislove, and W. Toorop. 2017. The Root Canary: Monitoring and Measuring the DNSSEC Root Key Rollover. In *Proceedings of SIGCOMM Posters and Demos '17, Los Angeles, CA, USA, August 22–24, 2017,* 2 pages.
https://doi.org/10.1145/3123878.3123890


*SIGCOMM Posters and Demos '17, August 22–24, 2017, Los Angeles, CA, USA*

ACM ISBN 978-1-4503-5057-0/17/08…$15.00
https://doi.org/10.1145/3123878.3123890

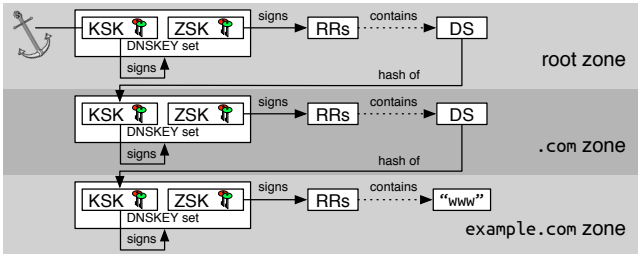


**Figure 1: Example DNSSEC chain of trust**

## 1 INTRODUCTION

The DNS Security Extensions (DNSSEC) enhance security by adding digital signatures to DNS records. DNS resolvers can validate these signatures to ensure that DNS records come from a legitimate source (authenticity) and have not been modified in transit (integrity). Validating DNS resolvers typically validate signatures along the so-called chain of trust. Figure 1 shows an example chain of trust, in this case for `www.example.com`. The most important takeaway from this example is that the chain of trust starts at the so-called Key Signing Key (KSK) for the root zone of the DNS. This key is called the 'trust anchor', and it is at the start of every chain of trust in the DNS. Validating resolvers only need to trust this key to verify signatures anywhere in the DNS, as long as there is a chain of trust from that signature all the way to the root zone of the DNS.

The current Root KSK was introduced when DNSSEC was enabled for the root zone in July 2010. Since then, the key has remained unchanged. This year, for the first time ever, this key will be replaced. This so-called *key rollover* is a standard practice in DNSSEC. Current best practices [1] recommend regularly replacing keys. The rollover of the Root KSK, however, is special, because it is also the trust anchor for the entire DNS. Validating DNS resolvers that rely on this key to validate signatures must pick up the new key, either through an automated process, or manual intervention. Resolvers that fail to pick up the new trust anchor will be unable to resolve *any* name in the DNS, regardless of whether or not it is DNSSEC signed. This is because signatures are validated from the root down; if a signature at root level fails to validate, anything below that level is also treated as untrusted (or 'bogus' in DNSSEC terms). Thus, this has a catastrophic impact for users and operators of these resolvers.

This paper presents the "Root Canary", a system to monitor and measure the impact of the Root KSK rollover. The Root Canary uses three different active measurement platforms to observe the impact of the Root KSK rollover on validating DNS resolvers across the Internet. Like a virtual canary-in-the-coalmine, the Root Canary serves as a near real-time warning system that signals if resolvers experience problems during the rollover. In addition to this, the Root Canary collects valuable longitudinal datasets that gauge the

| Measurement Platform | Frequency | #Vantage Points | Control over VPs | DNSSEC Algorithms |
|---|---|---|---|---|
| APNIC (Google Ads) [2] | Variable★ | 1000s/hour★ | No | RSA+ECDSA |
| Luminati [3] | Hourly†/Daily | 20M | Partial | All° |
| RIPE Atlas [4] | Hourly | 10k‡ | Yes | All° |

★Variable frequency and vantage points based on where advertisements are served.
†Hourly frequency around key dates in the rollover process (limited by cost).
‡Potentially biased towards vantage points operated by knowledgeable Internet users.
°See https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

**Table 1: Comparison of measurement methods**

impact of the rollover over the entire duration of the process from July 2017 until March 2018. We will analyse these datasets after the rollover completes, to draw lessons that can inform policy and best practices for future key management of the DNS root zone. The remainder of this paper presents and motivates our approach.

## 2 APPROACH

**Goals** – The Root Canary project has three goals. First, to provide an Internet-wide perspective on the impact of the Root KSK rollover. Second, to generate timely warnings when observed DNS resolvers experience problems. Finally, to collect high-quality longitudinal measurements that allow us to analyse the impact of the Root KSK rollover over the entire duration of the process.

**Existing approaches** – There are a number of existing approaches to measure DNSSEC validation. All of these, however, have limitations. Table 1 compares three platforms currently in use to measure and monitor DNSSEC validation. The first column compares the measurement frequency. As the table shows, this frequency depends on factors such as ad-placement strategies for Google Ads, and measurement cost. The second column provides an estimate of the number and distribution of measurement vantage points. The third column indicates the level of control over vantage points. Finally, the fourth column indicates which DNSSEC signing algorithms can be tested using each platform.

**Methodology** – The three approaches outlined above provide complementary visibility into the DNSSEC ecosystem. In this work, we are the first to combine all of them to provide the broadest possible coverage of the root key rollover. We will standardise measurement output in a format usable with existing tool chains. Since each of the three platforms has specific characteristics in terms of measurement dynamics and output, this is challenging. To give an example: measurements with RIPE Atlas probes require little post-processing, which makes it possible to provide almost instantaneous reporting on resolvers with problems. The output of the Luminati measurements require post-processing to correlate data recorded at different locations (from a webserver, and from authoritative name servers). This delays signalling of problems, and requires additional post-processing to make the output comparable to Atlas measurements.

**Measurement Phases** – The Root KSK rollover is a structured process that takes around nine months. We will perform continuous measurements with all three platforms for the entire duration of the process. Measurements are spread over six phases, corresponding to key milestones in the Root KSK rollover process. Figure 2 shows the phases, with milestones highlighted using orange circles. We will increase the measurement frequency around milestones, for those platforms that allow control over this frequency.

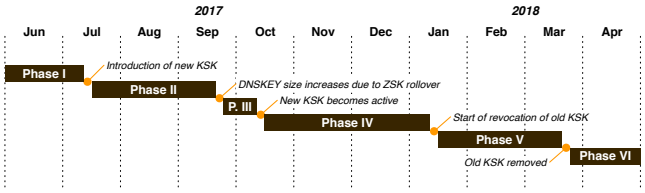


**Figure 2: Measurement phases**

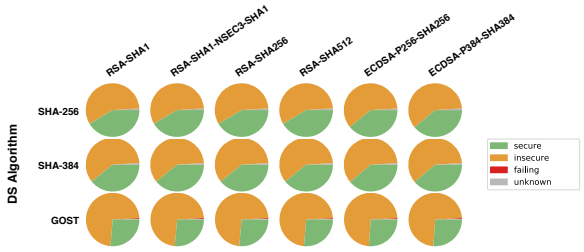


**Figure 3: Preliminary results for RIPE Atlas measurement**

**Reporting** – One of the key goals of this project is to provide near real-time information about the state of DNSSEC validation during the Root KSK rollover process. To make this possible, we intend to extend the DNSThought portal[1], that can visualise DNS resolver measurements using data from the RIPE Atlas platform.

**Analysis after the rollover** – The Root KSK rollover completes in March 2018. The datasets collected using the three platforms will then be used to perform analyse the entire process. A key goal of this study is to evaluate if any of the risks identified by the Root KSK rollover design team led to actual problems [5].

## 3 PRELIMINARY RESULTS

The measurement using RIPE Atlas probes has started. Figure 3 shows preliminary results for this measurement on the day after the introduction of the new Root KSK. The figure shows what fraction of probes perform DNSSEC validation for different signing algorithms. Note that, so far, the results show no probes failing as a result of the introduction of the new Root KSK. We are currently working on implementing the Luminati measurements, to further extend coverage of validating resolvers. We have also set up a project website[2], which presents results as they become available.

**Acknowledgements** – This work is supported by SURF, the Netherlands collaborative organisation for higher education and research, and in part by NSF grants CNS-1421444 and CNS-1563320.

## REFERENCES

[1] O. Kolkman, W. Mekking, and R. Gieben. RFC 6781 - DNSSEC Operational Practices, Version 2, 2012.
[2] Geoff Huston. Measuring DNSSEC Use. In *APNIC 36 Conference*, Xi'An, China, 2013.
[3] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In *Proceedings of USENIX Security '17*, Vancouver, BC, Canada, 2017.
[4] RIPE NCC. RIPE Atlas, 2017.
[5] ICANN. Root Zone KSK Rollover Plan. 2016.

[1] https://github.com/DNS-OARC/ripe-hackathon-dns-caching
[2] https://rootcanary.org/