Roll, Roll, Roll Your Root

A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover

RoN++ Meeting 2019 – Utrecht, 2020-01-08

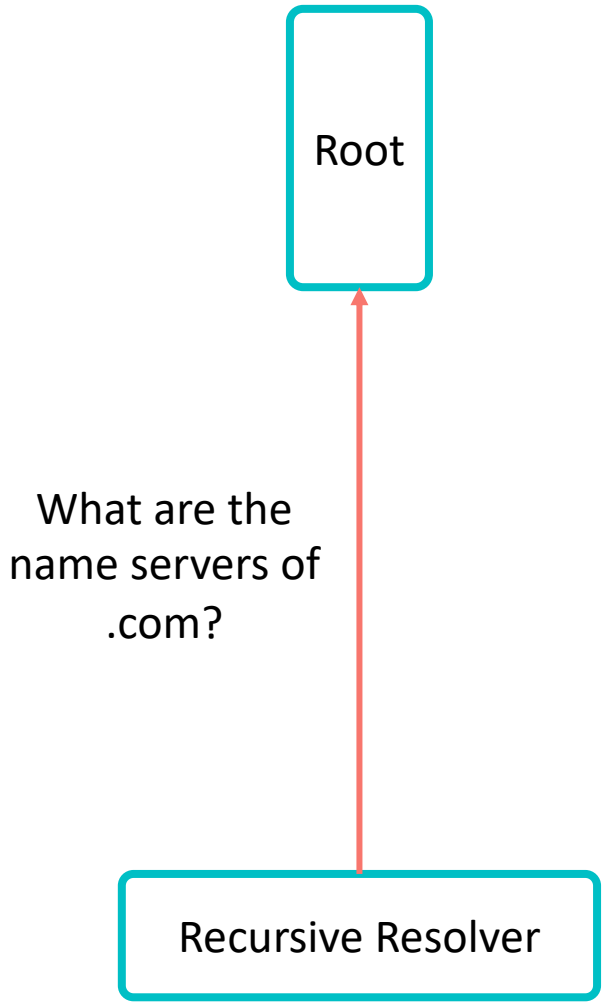
Moritz Müller[3,4], Matthew Thomas[6], Duane Wessels[6], Wes Hardaker[5], Taejoong Chung[2], Willem Toorop[1], Roland van Rijswijk-Deij[1,4]

[1]NLnet Labs, [2]Rochester Institute of Technology, [3]SIDN Labs, [4]University of Twente, [5]USC/Information Sciences Institute, [6]Verisign

Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or "*rolled*") for the *first time*

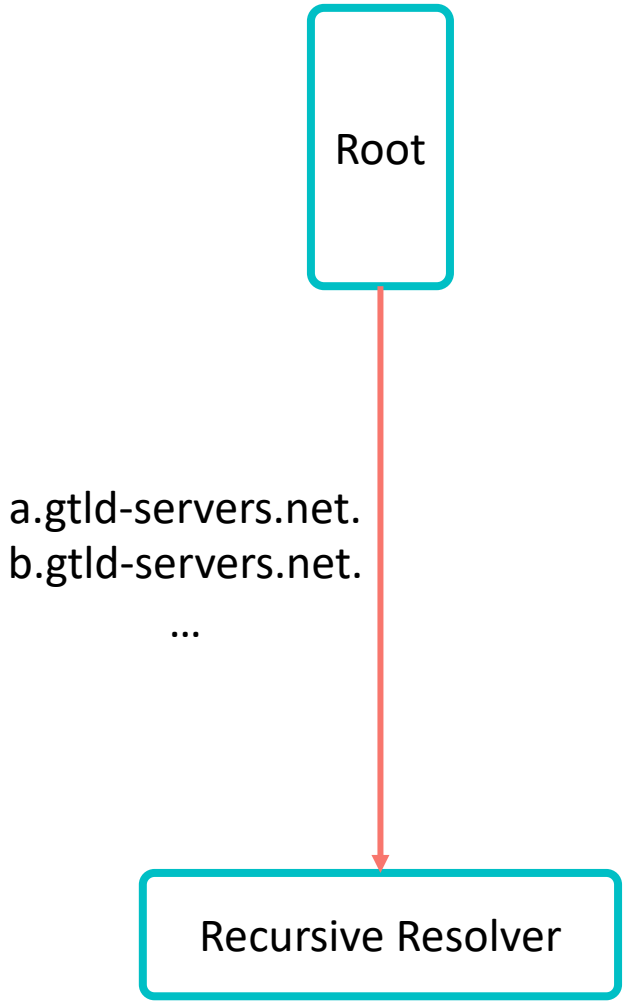
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or "*rolled*") for the *first time*

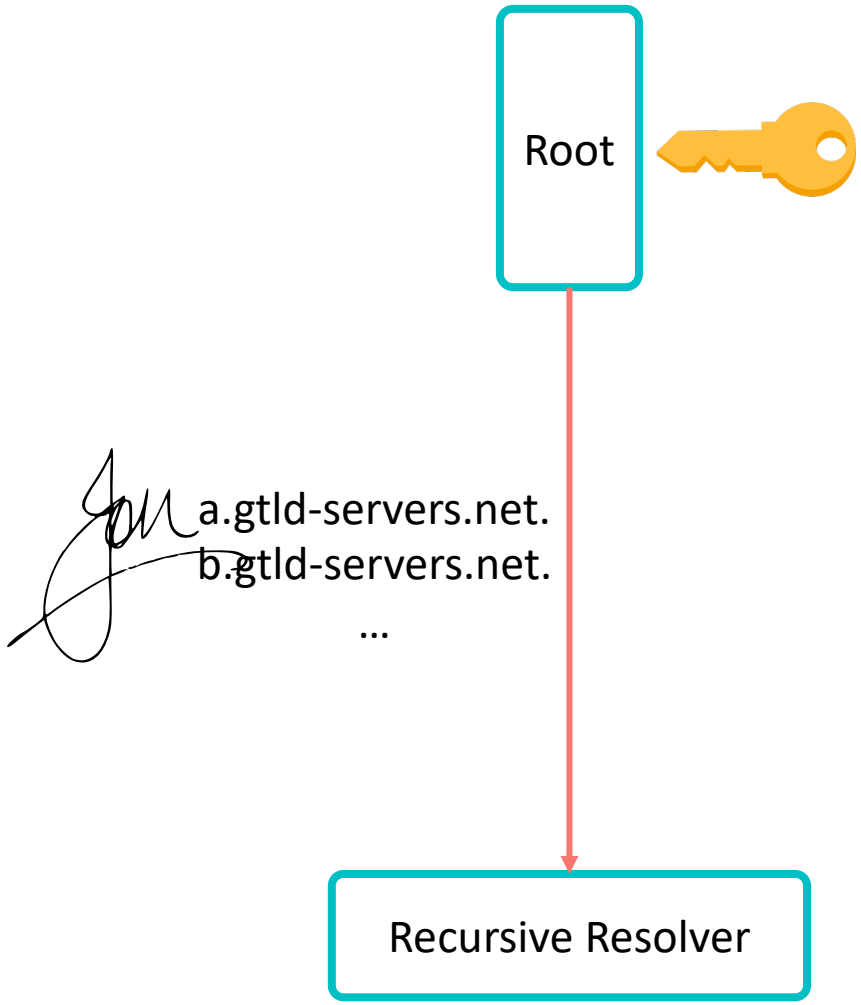
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or "*rolled*") for the *first time*

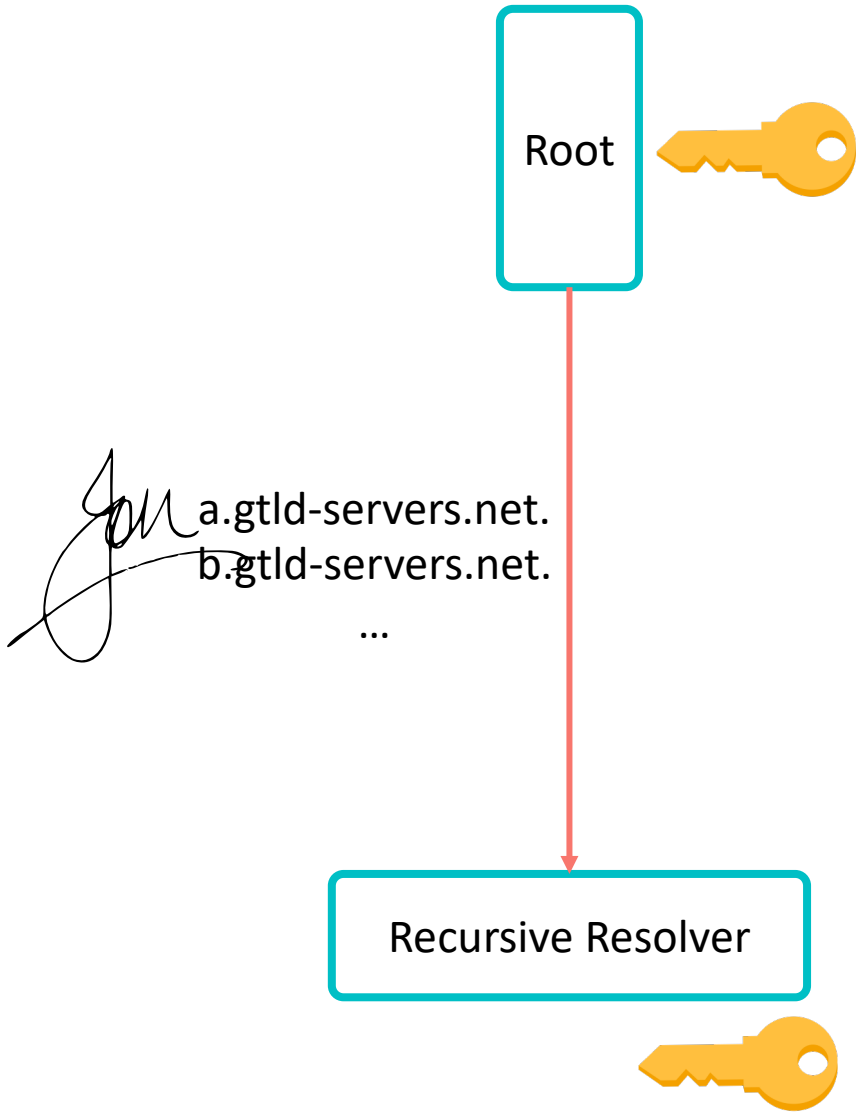
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or "*rolled*") for the *first time*

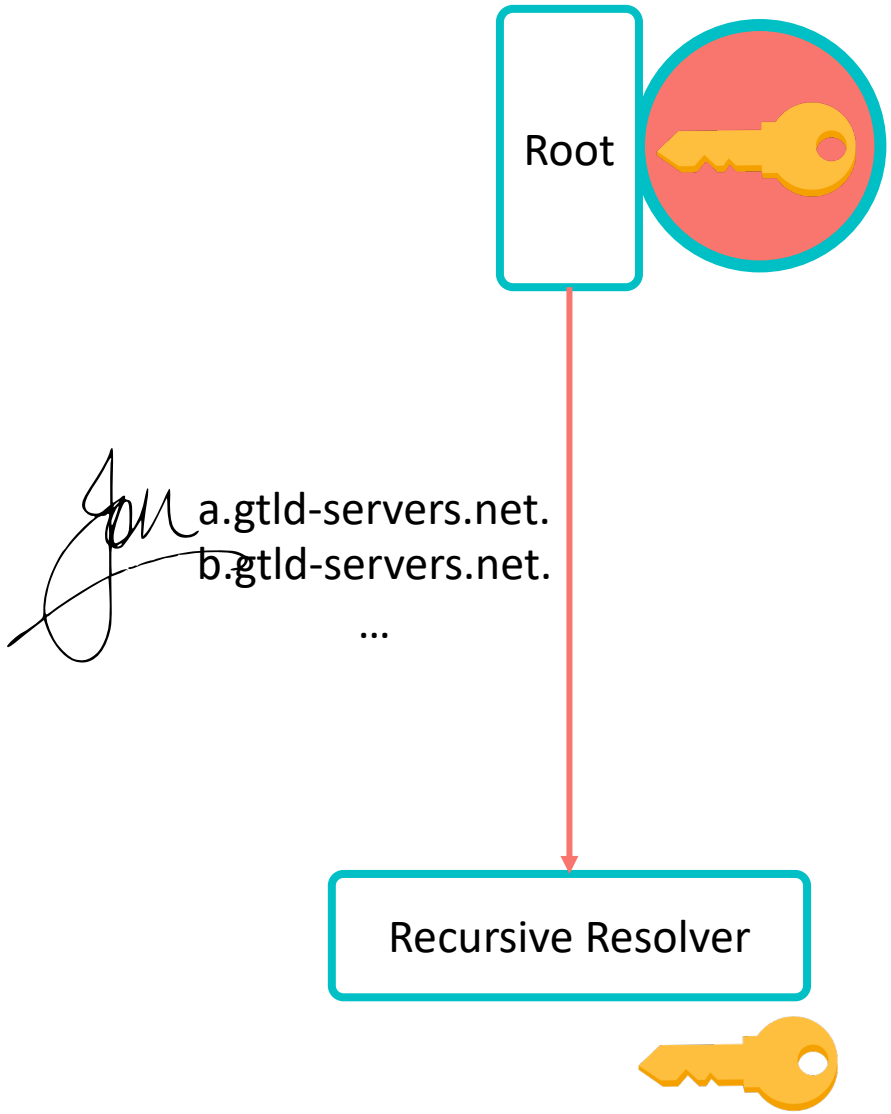
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or "*rolled*") for the *first time*

- The old key: **KSK-2010**
- The new key: **KSK-2017**

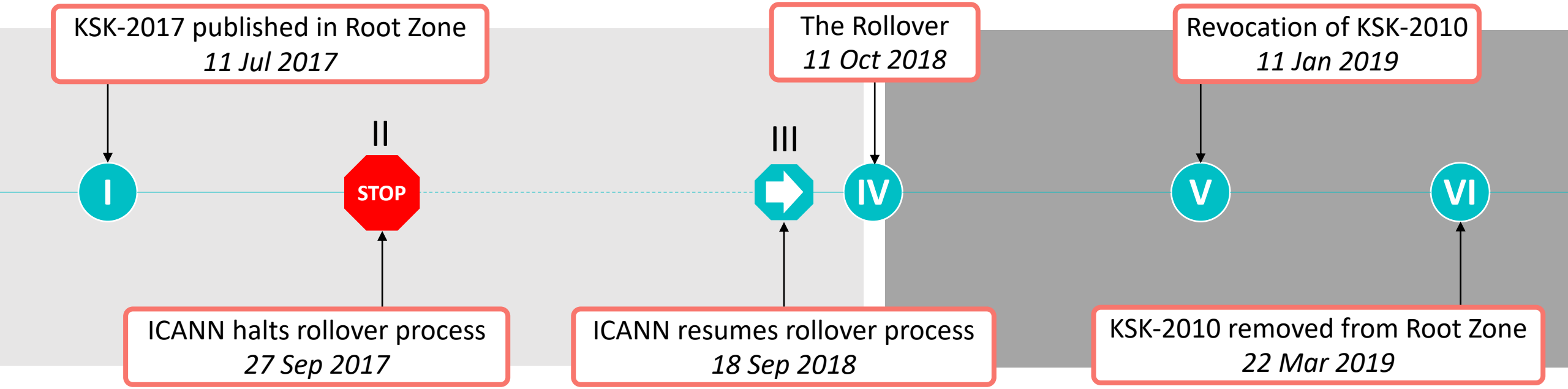


Why is rolling hard?

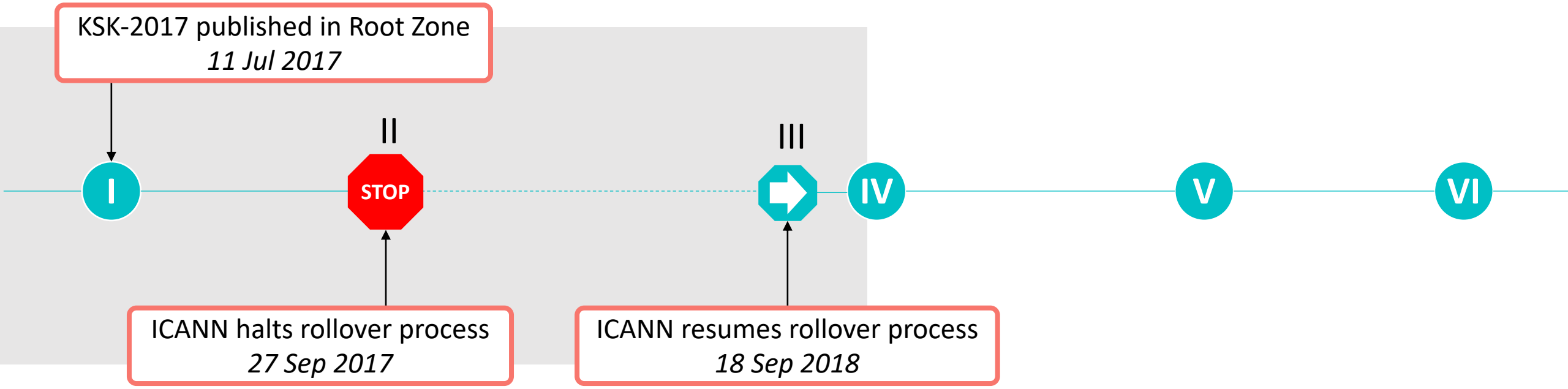
- No key → No validation → No DNS responses
- **Every** validator needs to have KSK-2017, but:
  - Validators use hard-coded keys
  - Containers challenge key update
  - People tend to forget about DNS

Photo by Icons8 team on Unsplash

Timeline

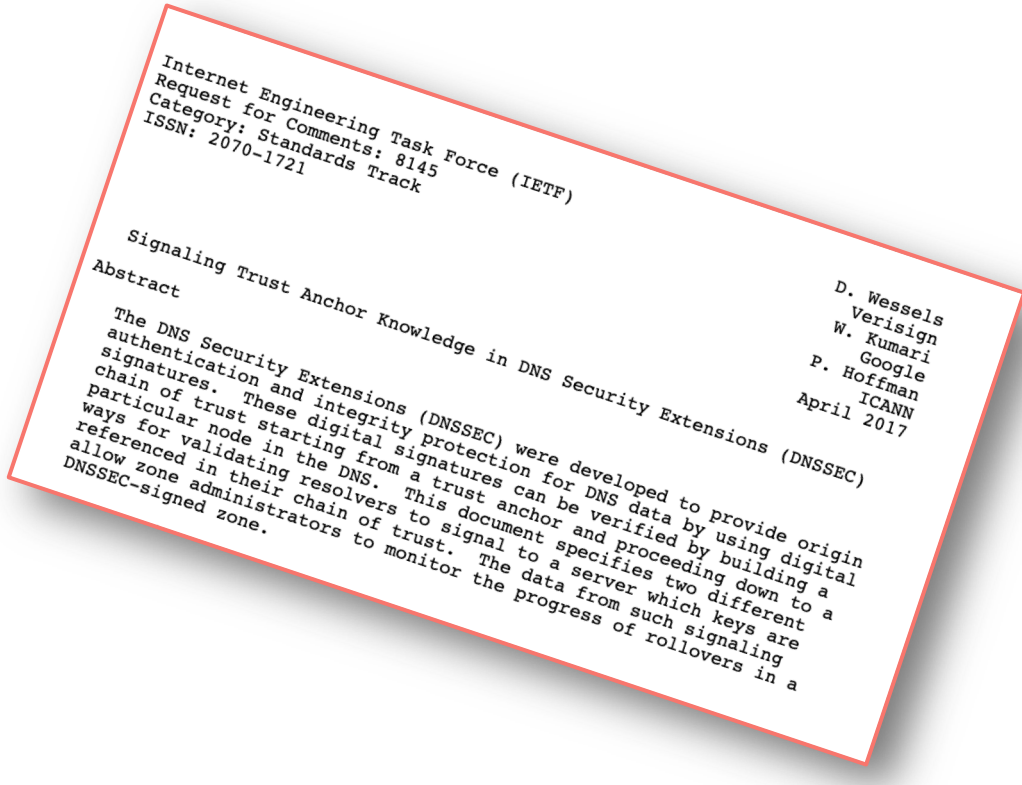

KSK-2017 published in Root Zone
11 Jul 2017
I
II
STOP
ICANN halts rollover process
27 Sep 2017
III
ICANN resumes rollover process
18 Sep 2018
The Rollover
11 Oct 2018
IV
Revocation of KSK-2010
11 Jan 2019
V
VI
KSK-2010 removed from Root Zone
22 Mar 2019

Before the Rollover



Resolver Telemetry: RFC 8145

- The goal: estimating how many validators had KSK-2017
- The solution: resolvers signal to the root which keys they trust



Internet Engineering Task Force (IETF)
Request for Comments: 8145
Category: Standards Track
ISSN: 2070-1721

D. Wessels
Verisign
W. Kumari
Google
P. Hoffman
ICANN
April 2017

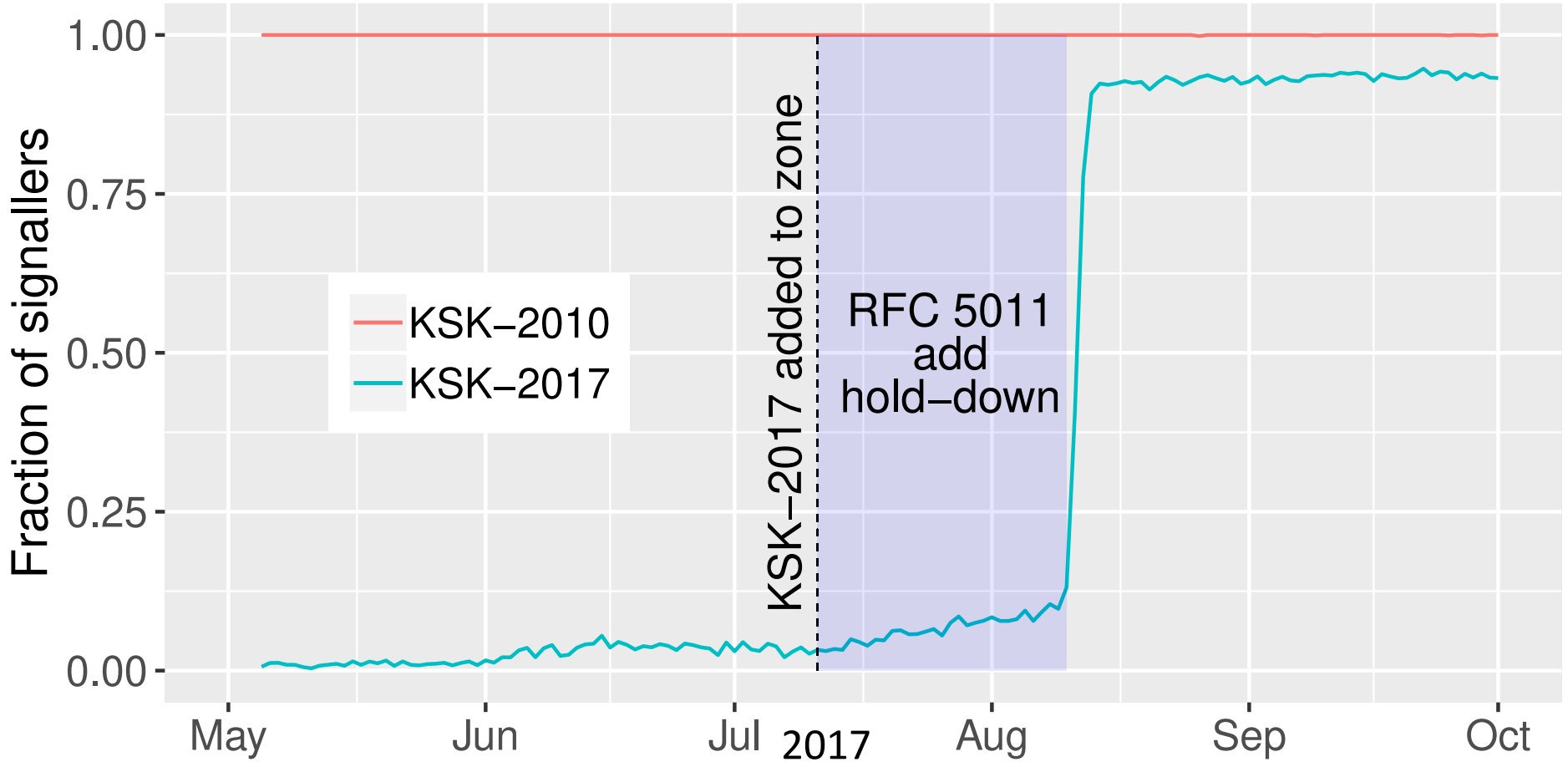
Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)

Abstract

The DNS Security Extensions (DNSSEC) were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. These digital signatures can be verified by building a chain of trust starting from a trust anchor and proceeding down to a particular node in the DNS. This document specifies two different ways for validating resolvers to signal to a server which keys are referenced in their chain of trust. The data from such signaling allow zone administrators to monitor the progress of rollovers in a DNSSEC-signed zone.

- Data from ICANN from A, B, and J root
- Signals from up to 100,000 validators daily

Uptake of KSK-2017



Uptake of KSK-2017

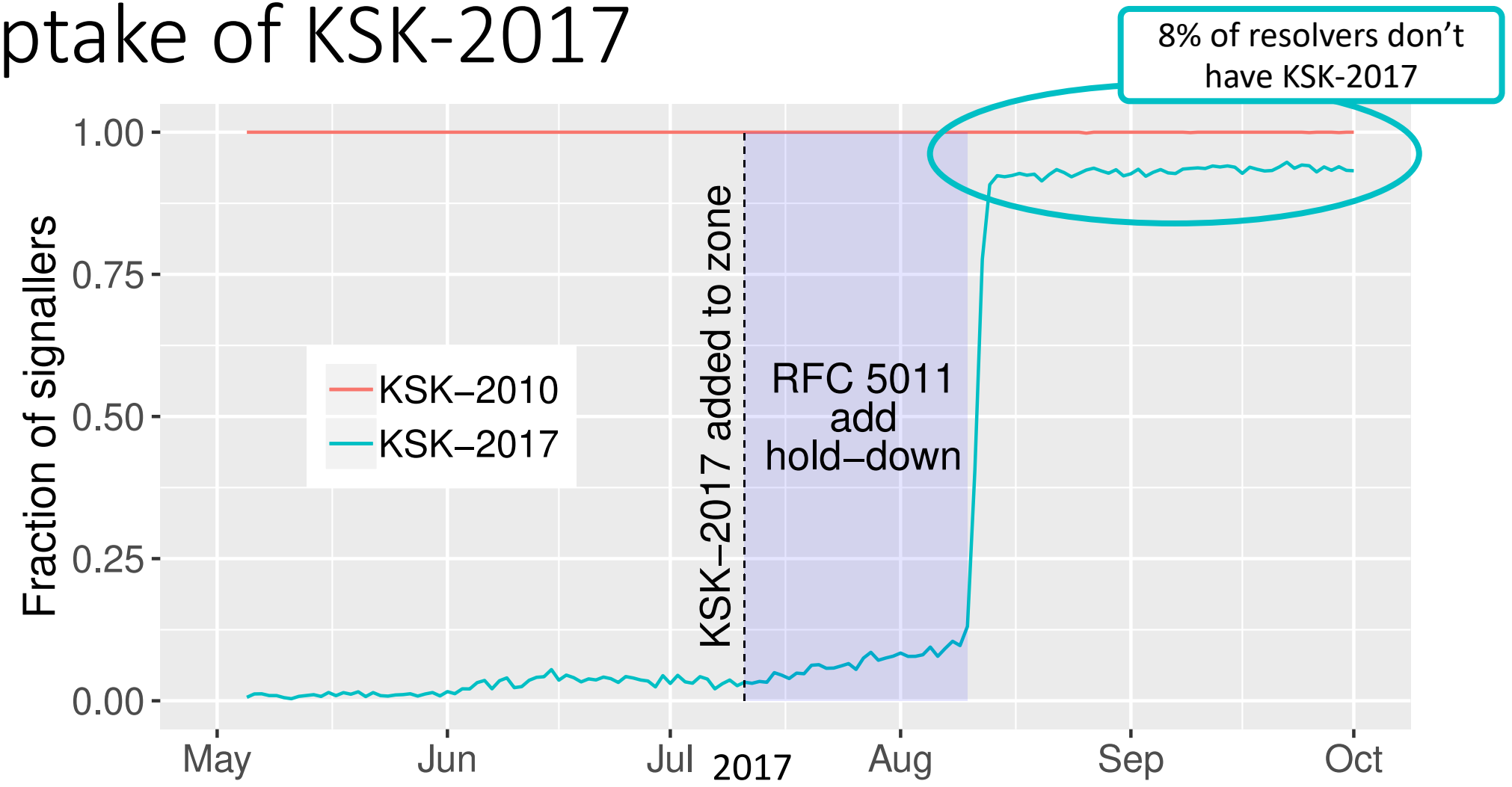


Photo by John Matychuk on Unsplash

I

STOP

IV

V

VI

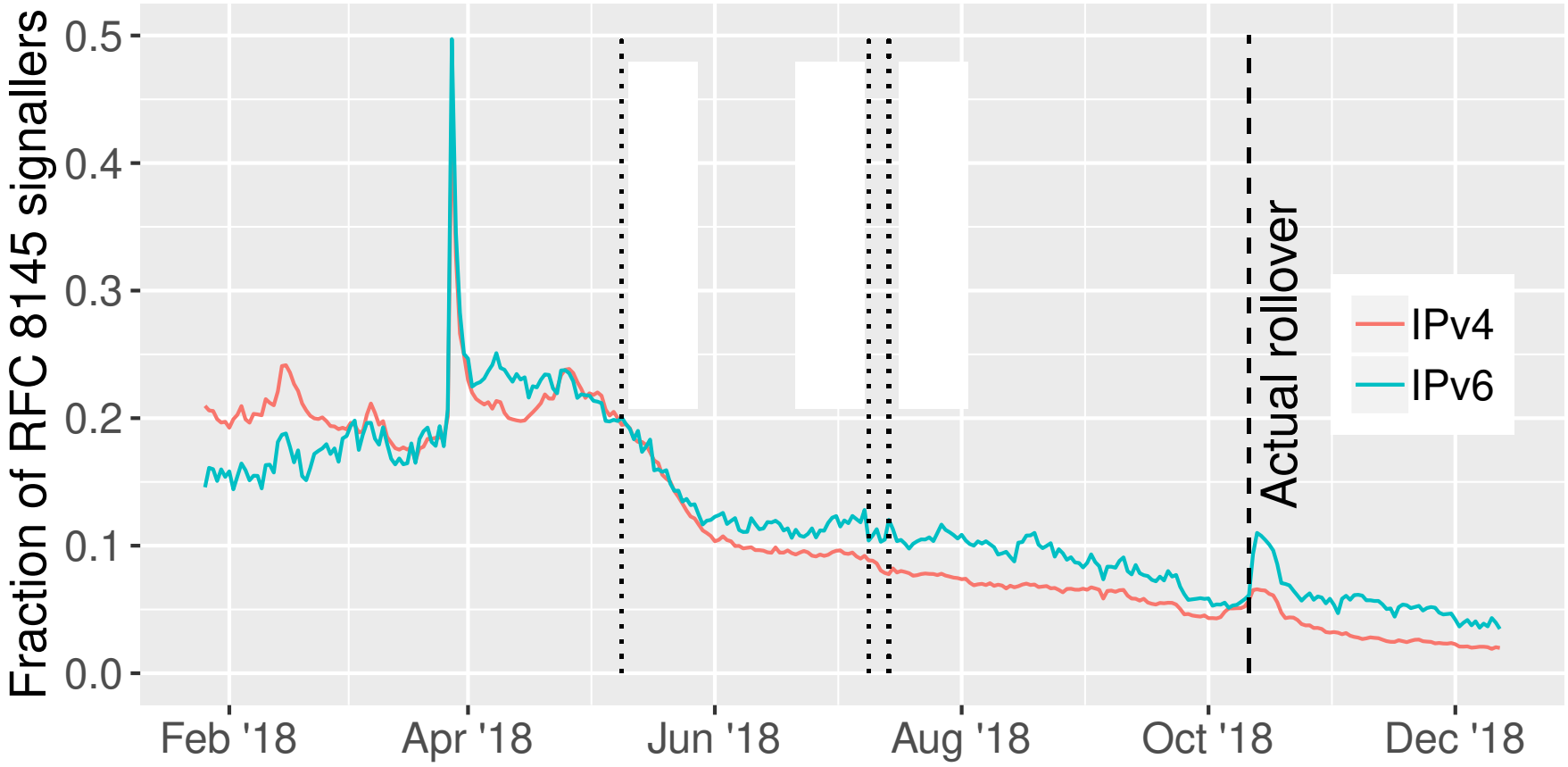
Zooming in on resolvers that only have KSK-2010

- Lots of RFC 8145 sources sent only one signal
- Many sent only a few queries

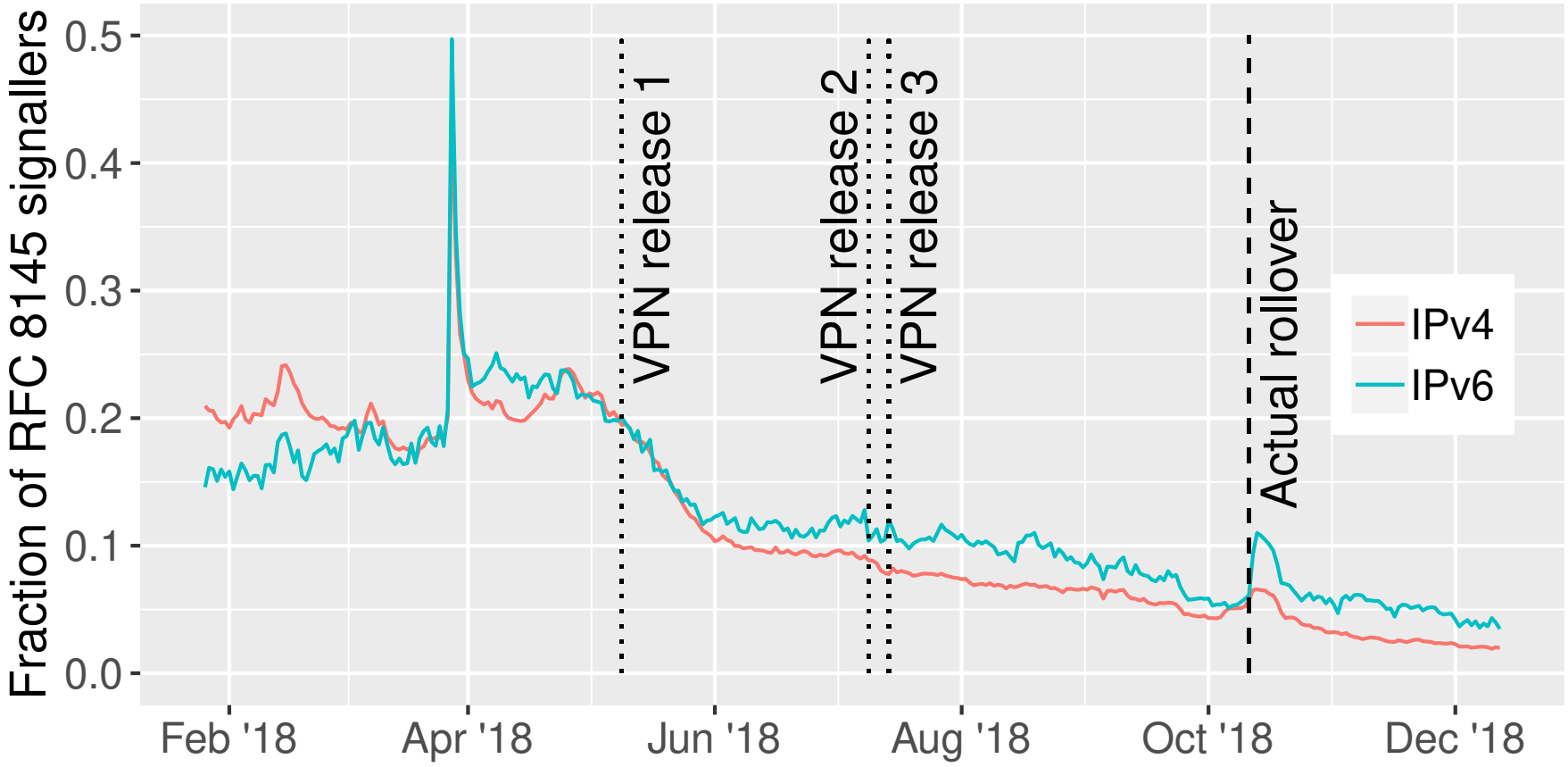
Query	Count
_ta-4a5c	15,447
.	9,182
VPN domain	3,156
VPN alternate domain	415
_sip._udp.otherdomain	86

Domains, queried by resolvers

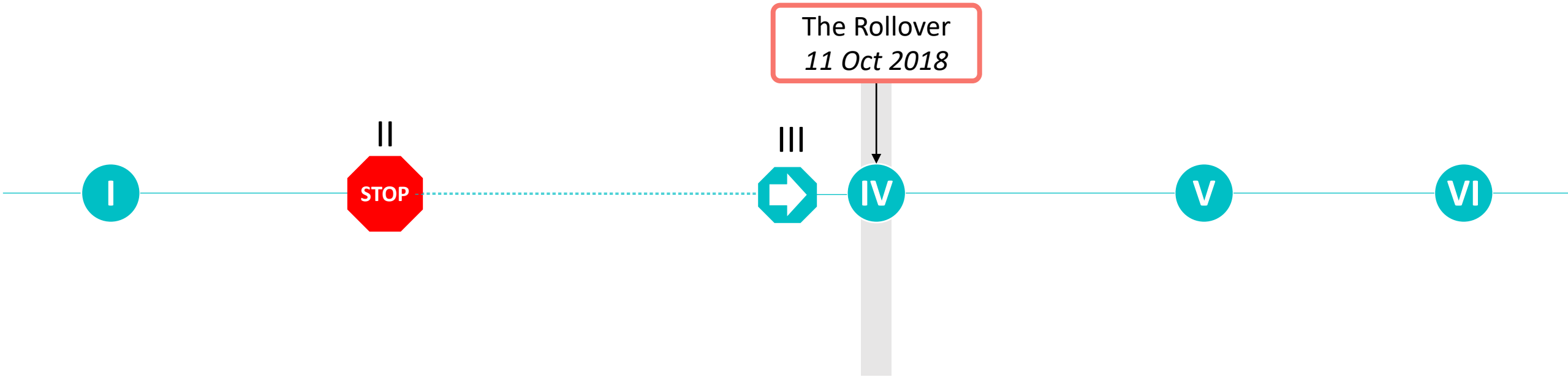
Zooming in on resolvers that only have KSK-2010



Zooming in on resolvers that only have KSK-2010



During the Rollover

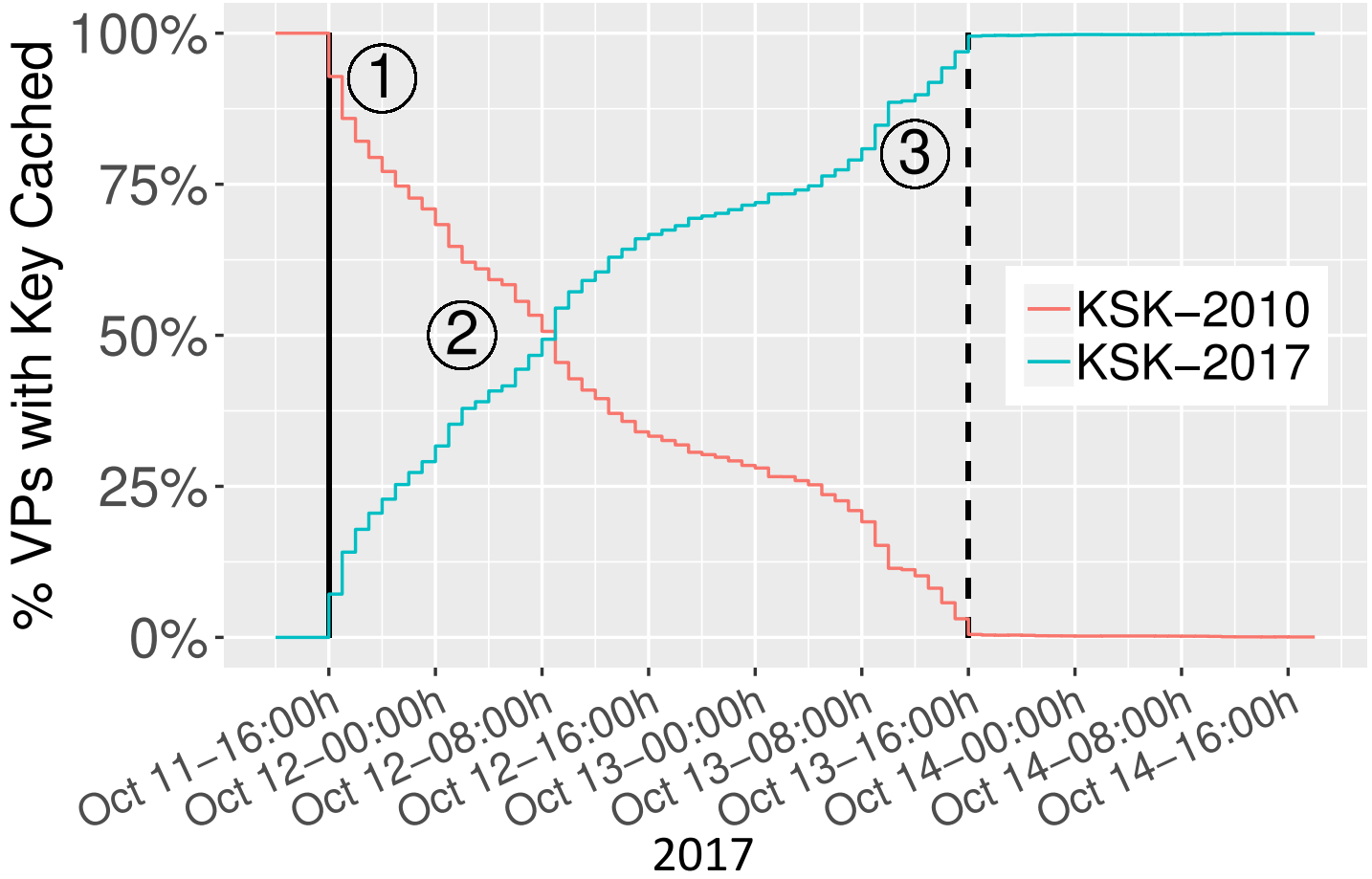


The User's Perspective: RIPE Atlas

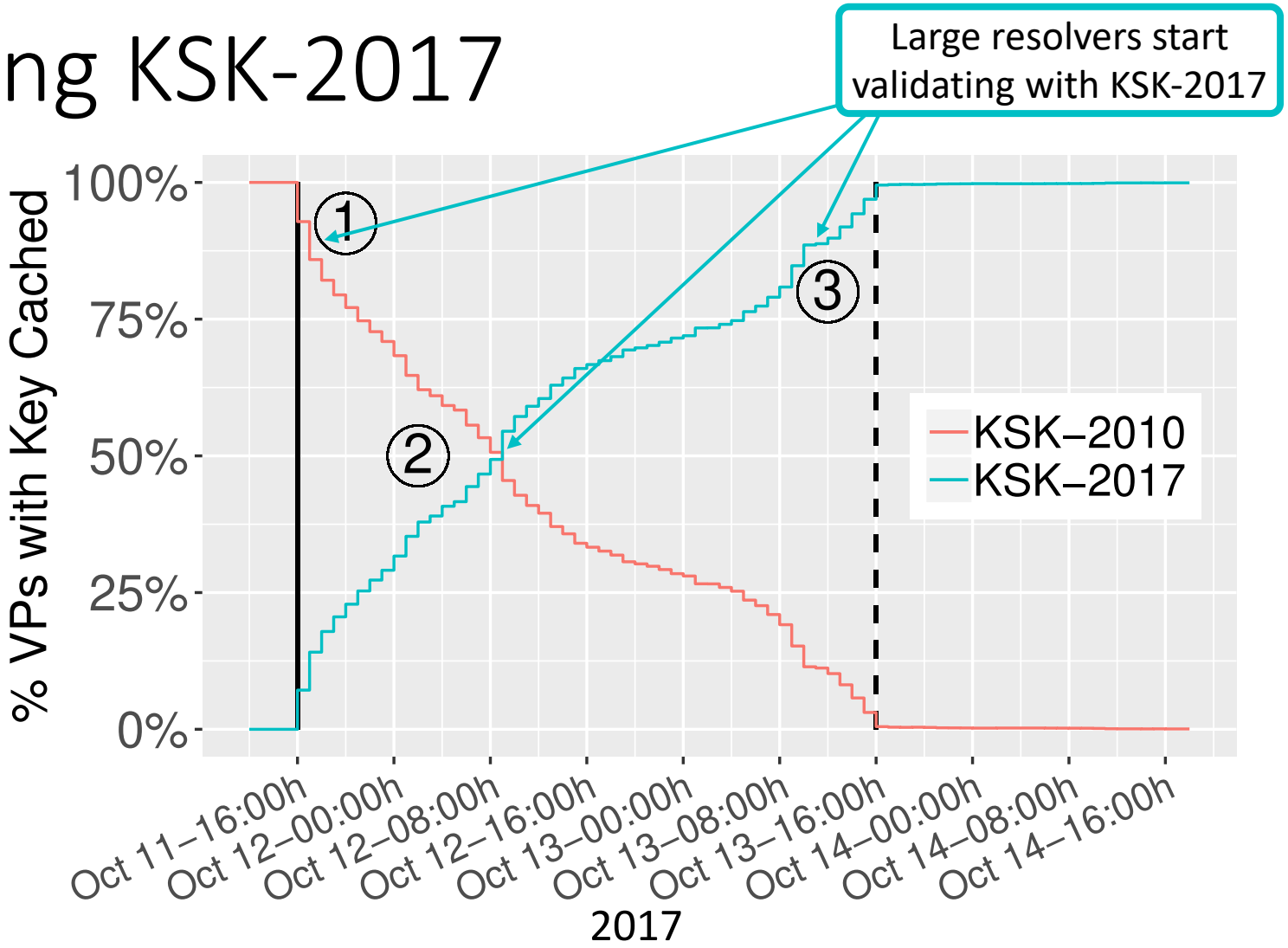
- The goal: measuring how **users** perceive the rollover
- The approach: Measuring with all RIPE Atlas probes once per hour
    a) If they have cached KSK-2017
    b) If they validate correctly

- We observed **35,719 resolver addresses** in **3,141 ASes** and correlated failing resolvers with DNSKEY queries with DITL data

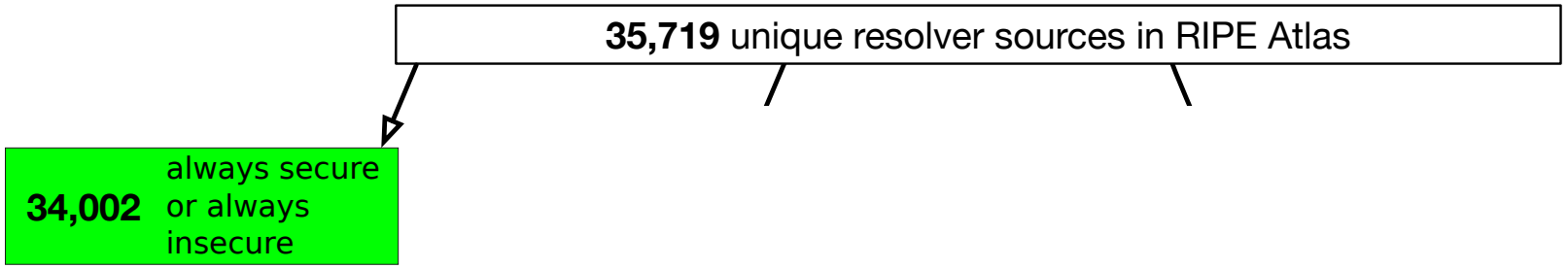
Activating KSK-2017



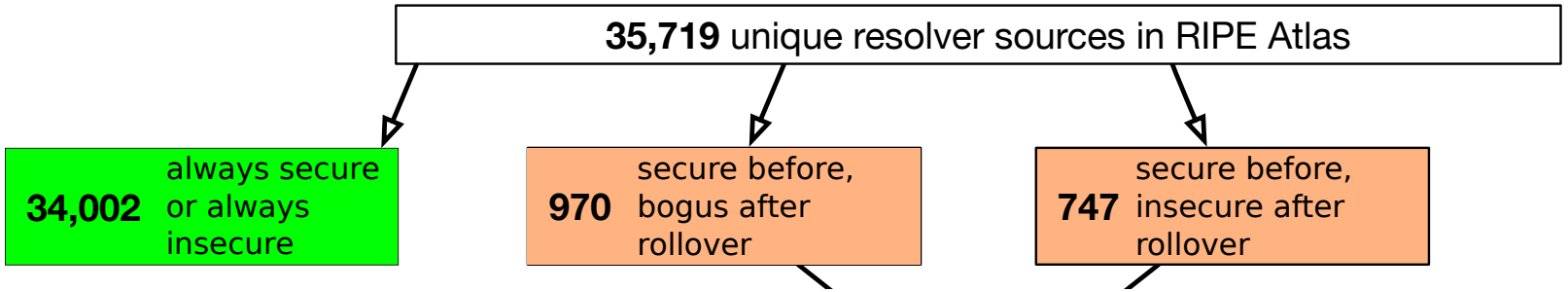
Activating KSK-2017



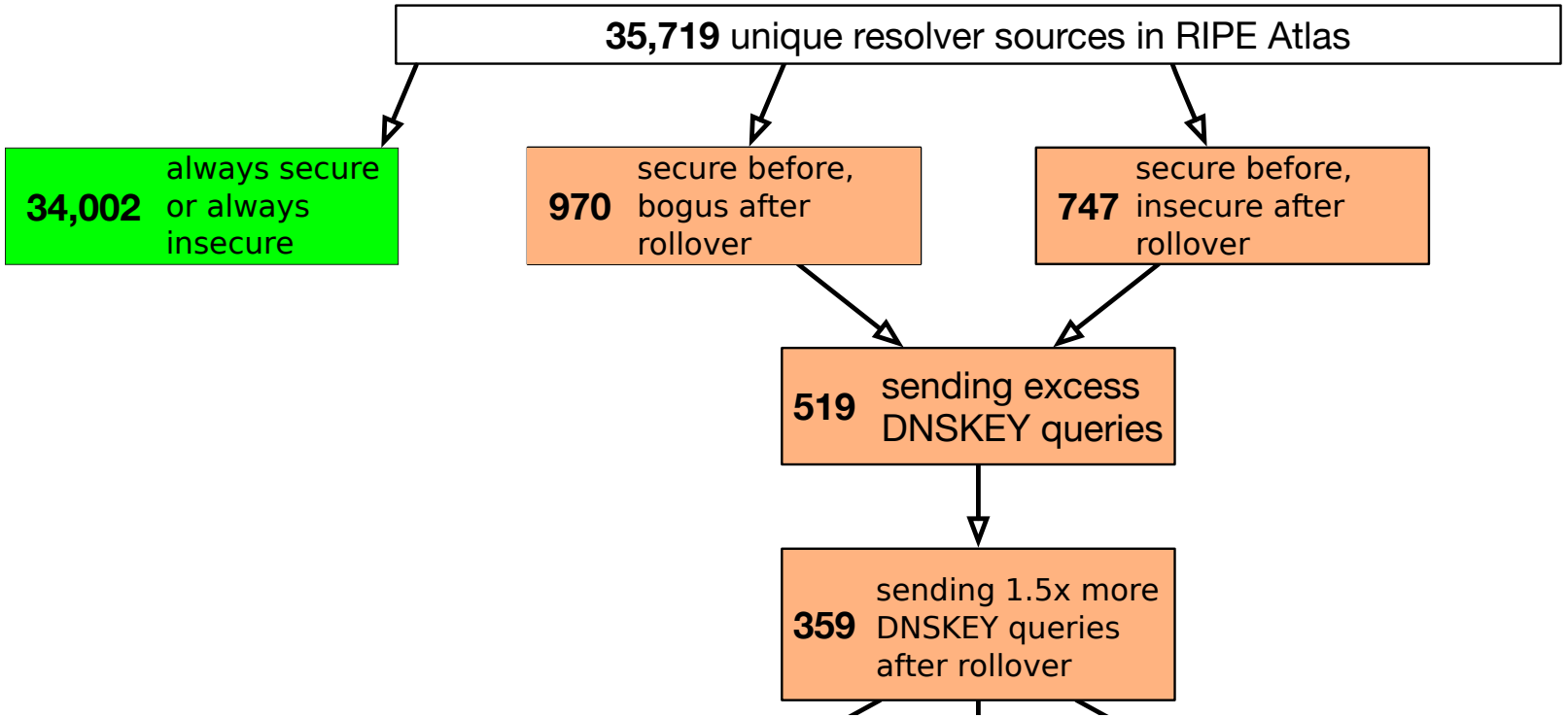
Reaction to Validation Failures



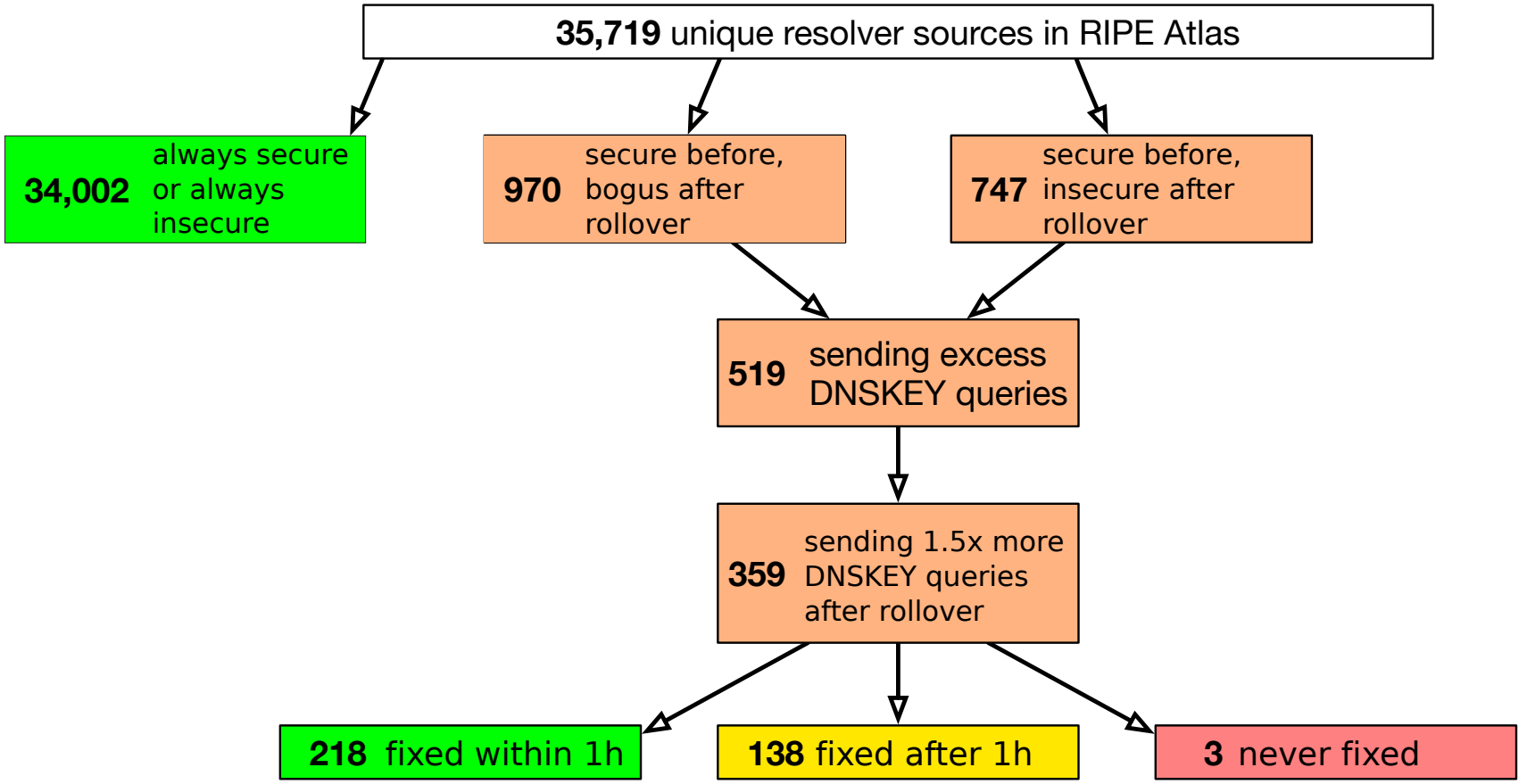
Reaction to Validation Failures



Reaction to Validation Failures



Reaction to Validation Failures



Broadband restored to Eir customers after outage

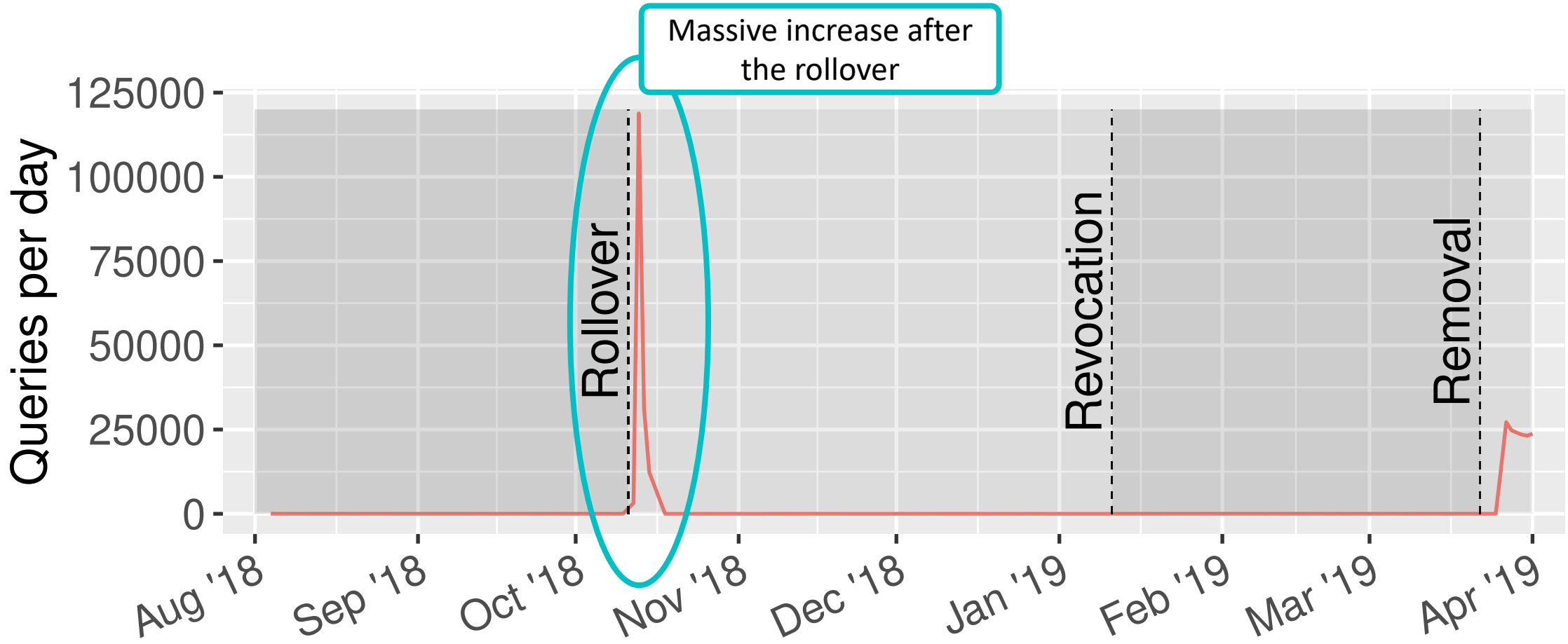
Company says problem with DNS server led to outage across the country

Sat, Oct 13, 2018, 21:23 | Updated: Sun, Oct 14, 2018, 07:55

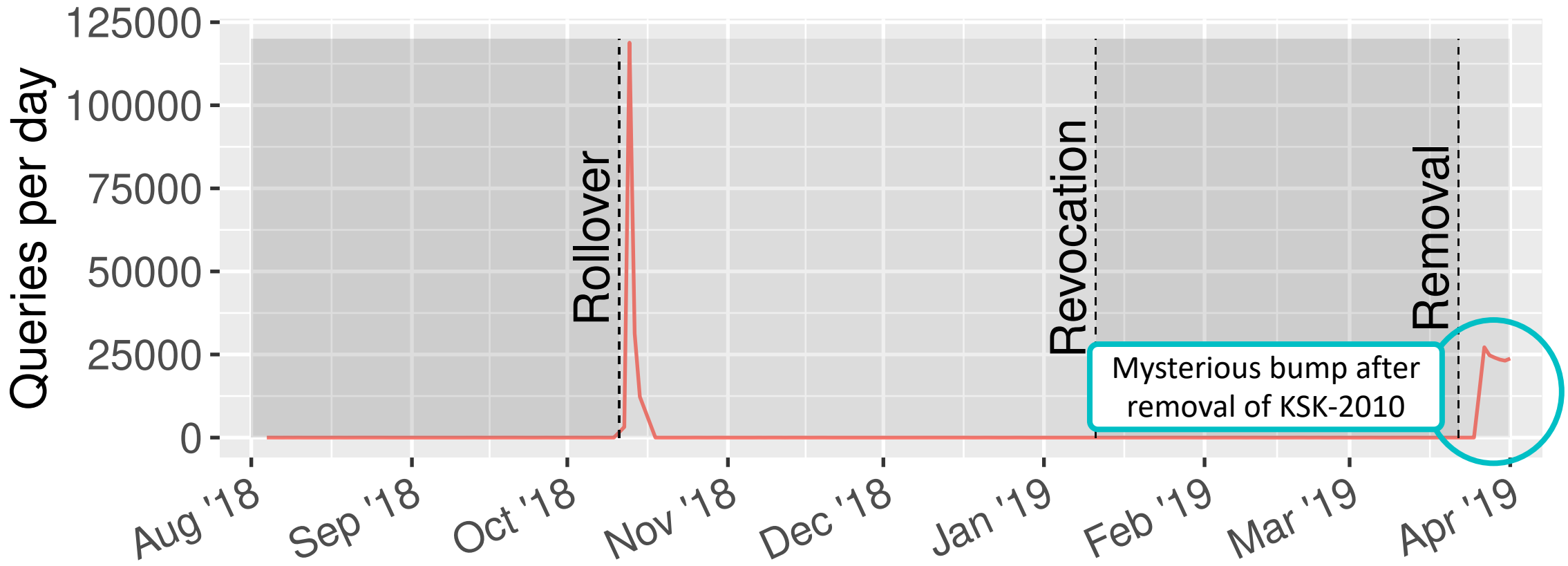
File photograph: Maxwells

https://www.irishtimes.com/business/technology/broadband-restored-to-eir-customers-after-outage-1.3663004

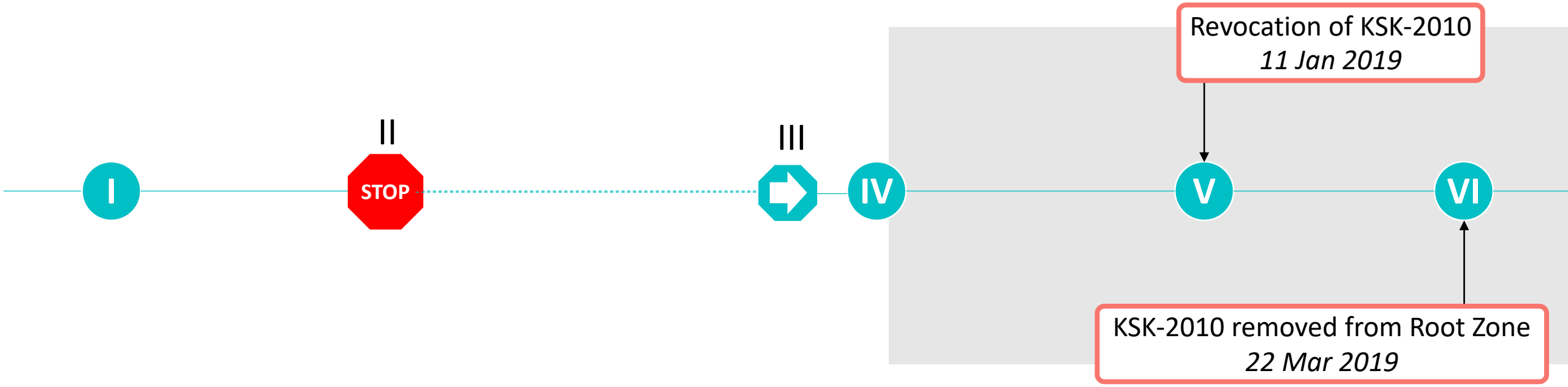
EIR Outage - Was it DNS(SEC)?



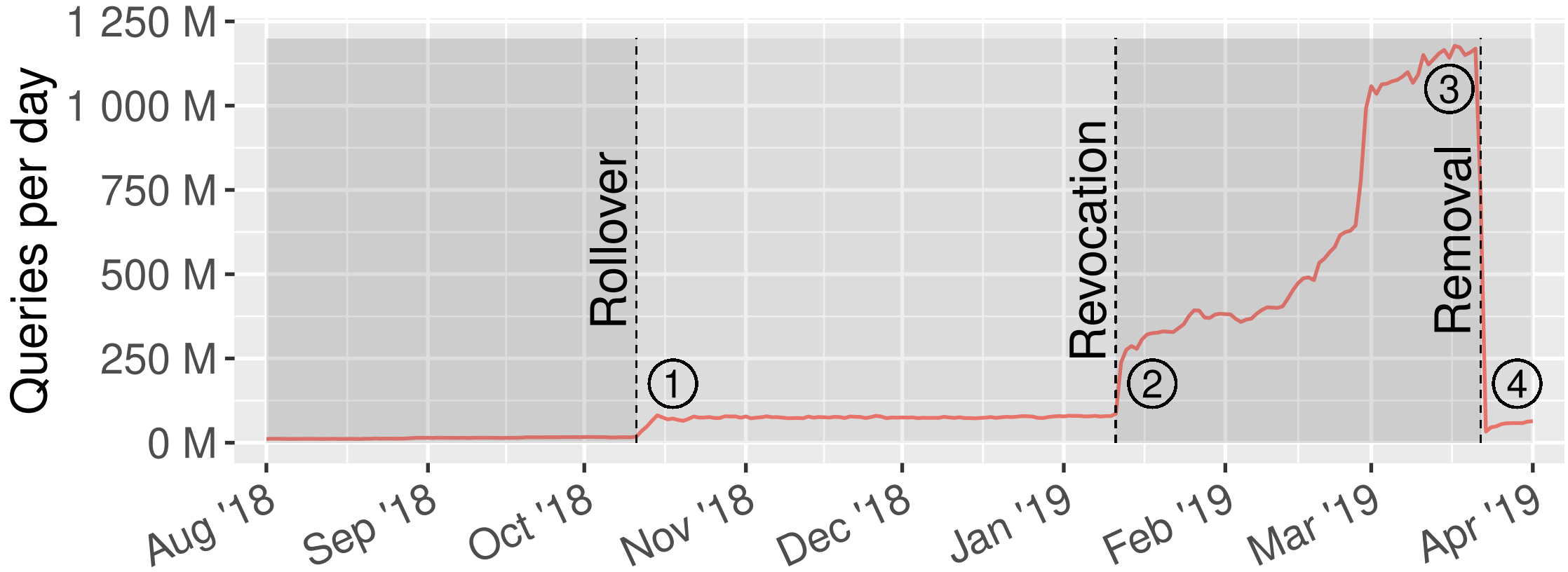
EIR Outage - Was it DNS(SEC)?



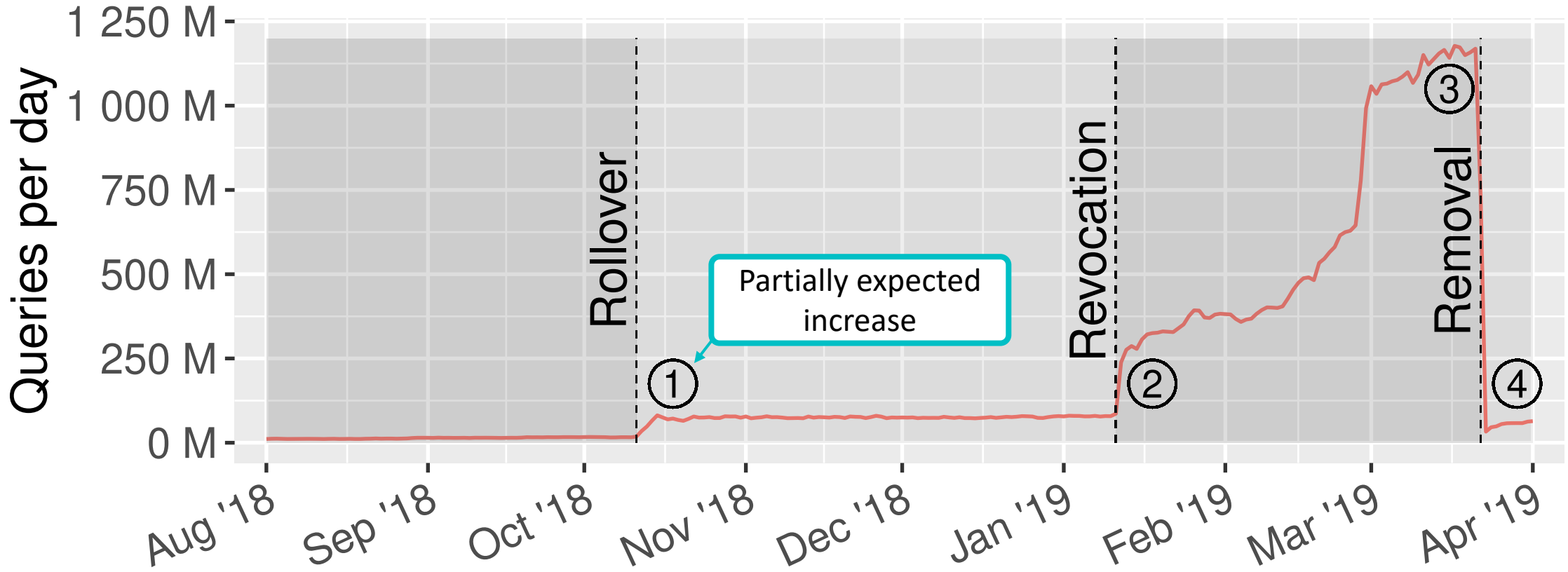
After the Rollover



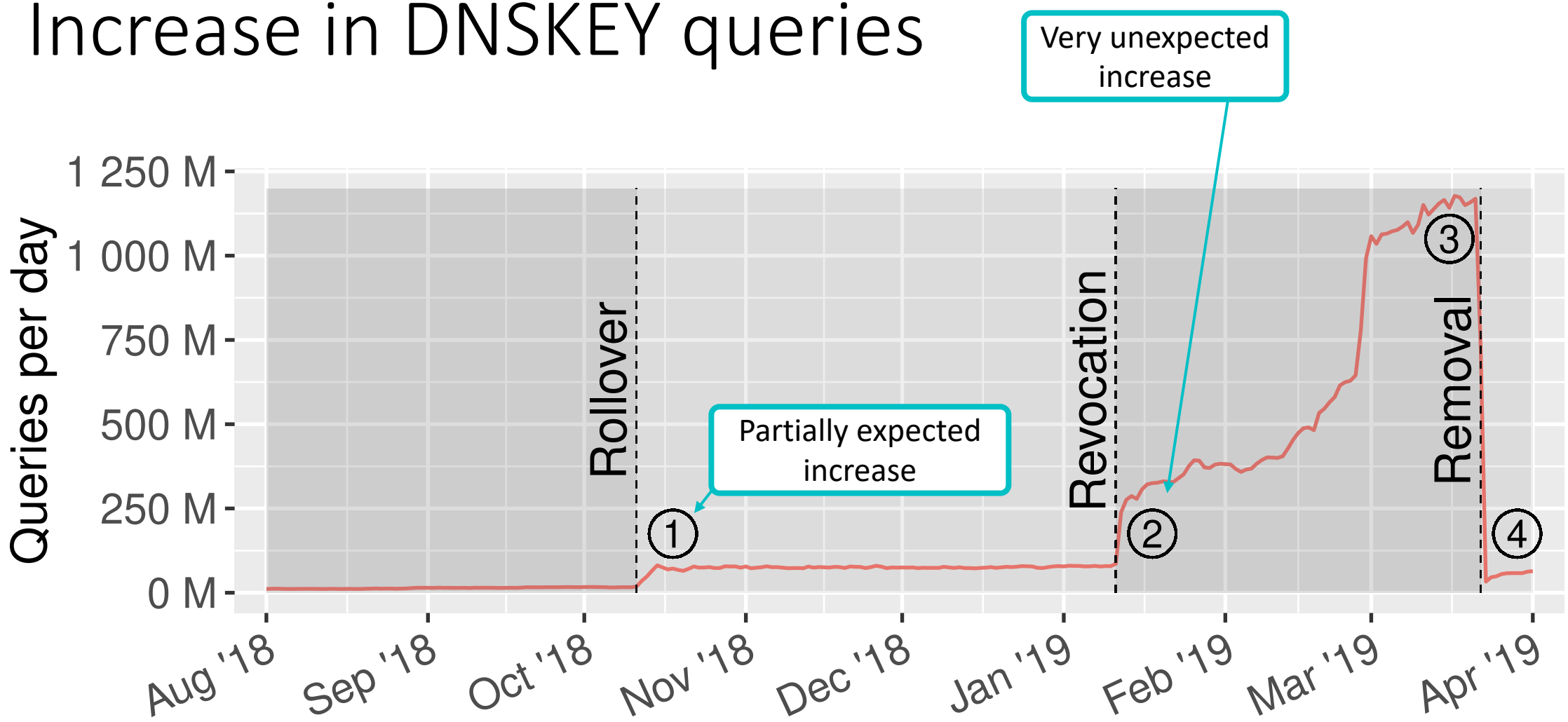
Increase in DNSKEY queries



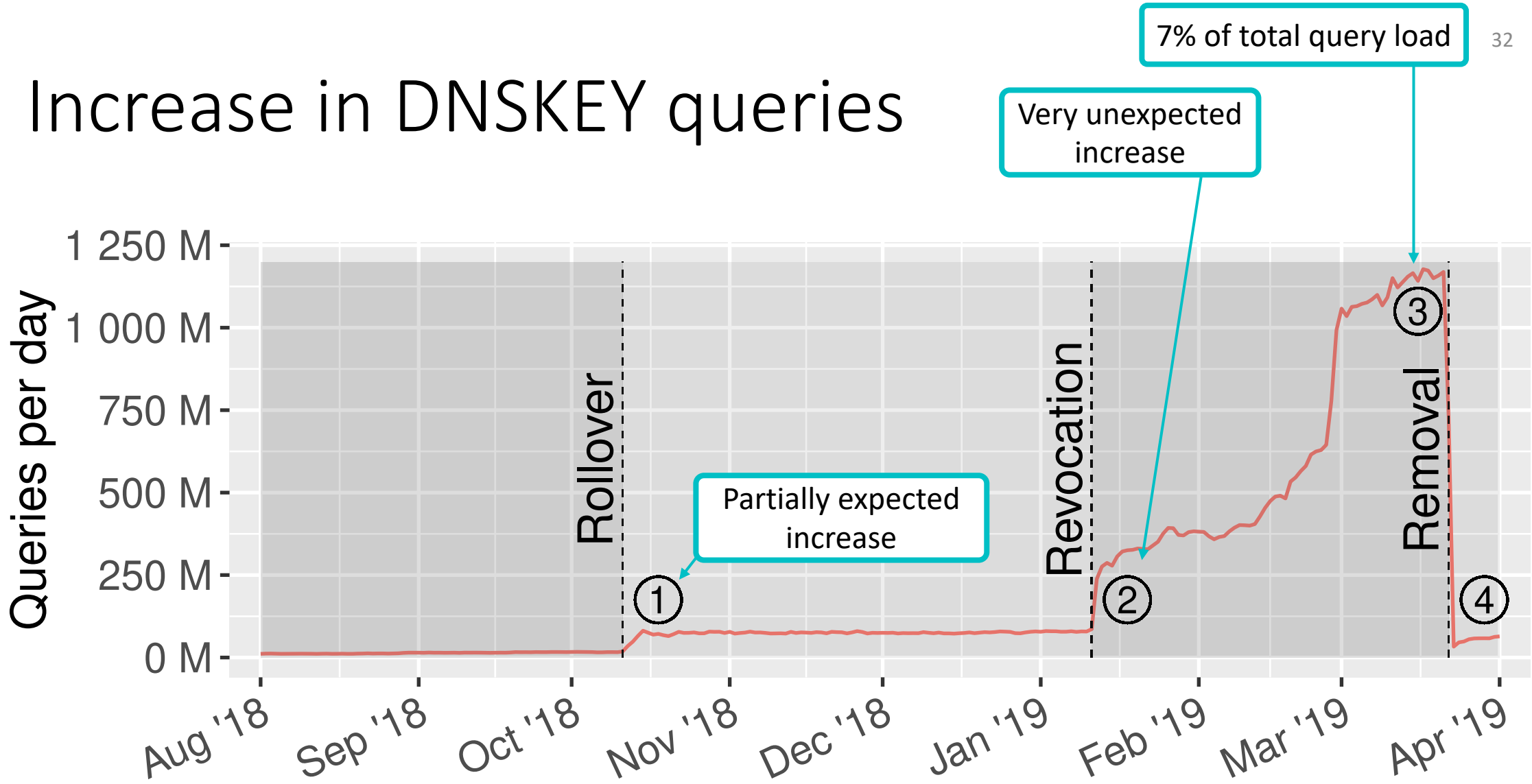
Increase in DNSKEY queries



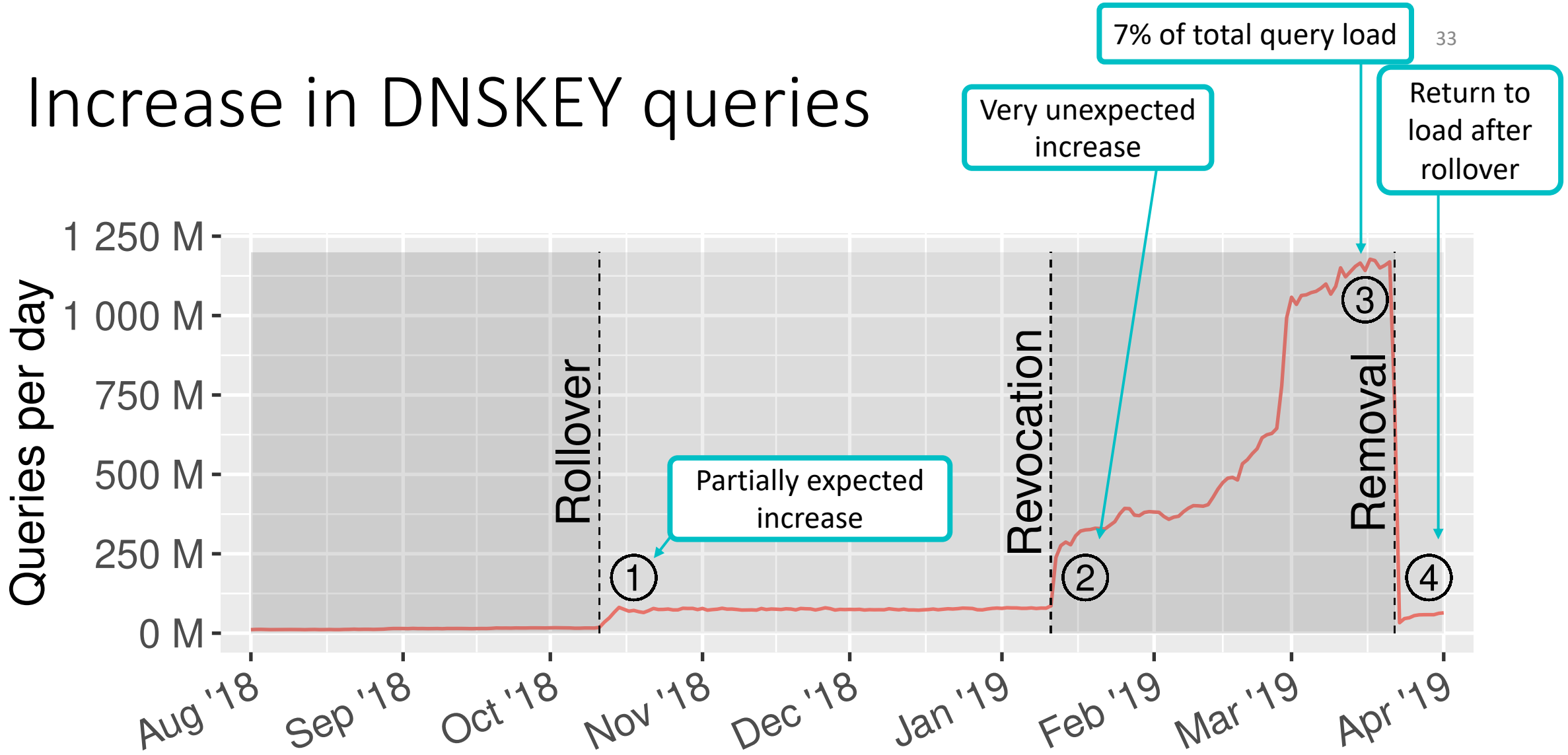
Increase in DNSKEY queries



Increase in DNSKEY queries



Increase in DNSKEY queries



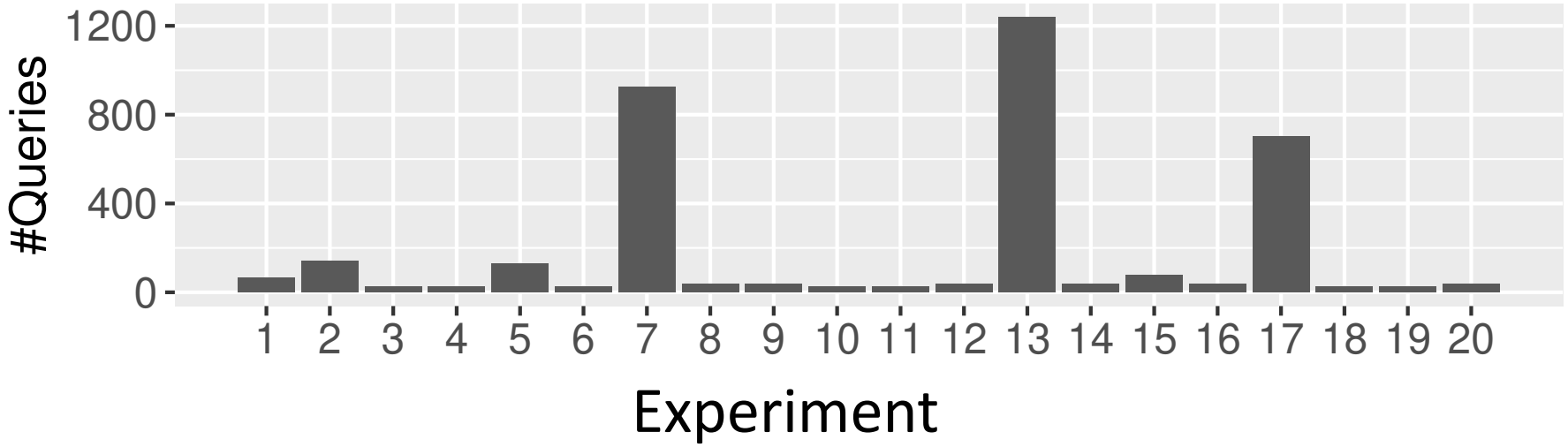
Who's behind the query floods?

- DNS CHAOS queries to sources reveal mostly older versions of BIND
- Outreach
  - A large French cloud hosting provider confirmed a source running BIND 9.8.2 on CentOS
  - Large midwestern university confirmed DNS lab exercise and provided BIND config

Photo by Kelly Sikkema on Unsplash

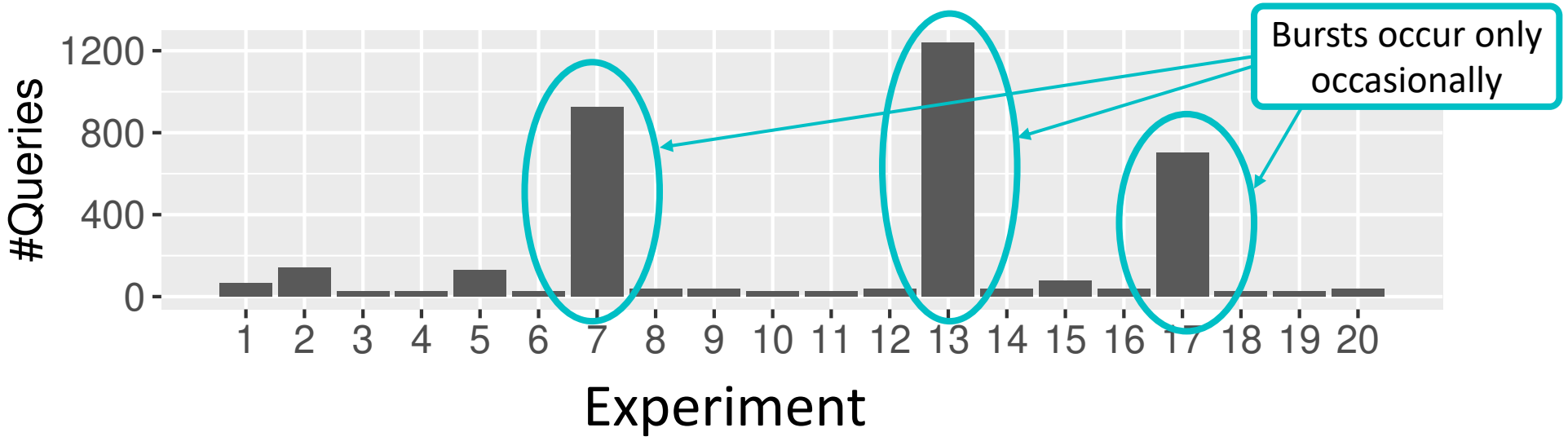
Reproducing Key Floods with BIND

- Conditions for reproducing DNSKEY floods with BIND:
  - DNSSEC managed keys contains KSK-2010, but not KSK-2017
  - The dnssec-enable flag was set to false
  - The dnssec-validation flag was unset, leaving it in its default state of “yes.”

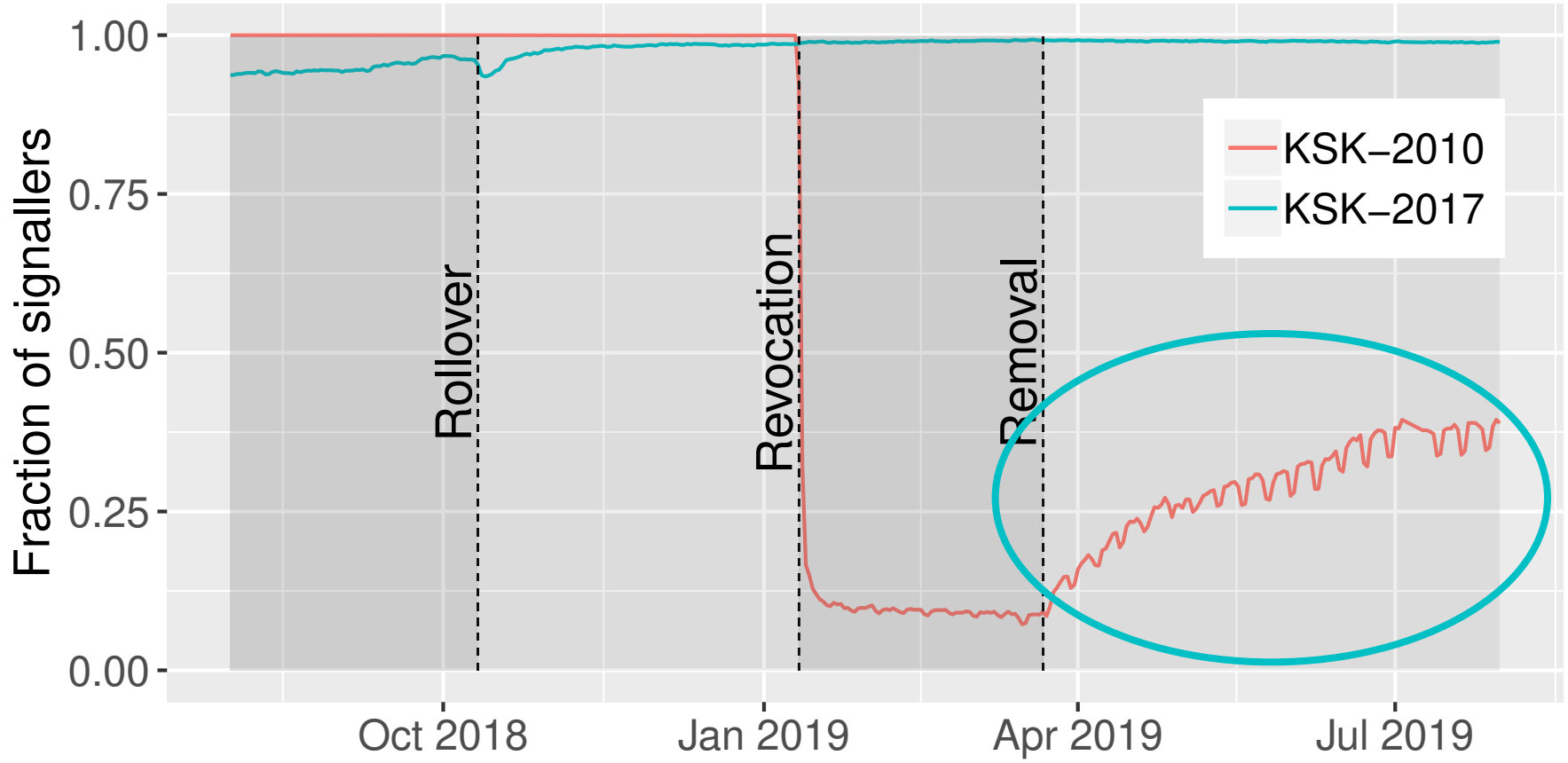


Reproducing Key Floods with BIND

- Conditions for reproducing DNSKEY floods with BIND:
  - DNSSEC managed keys contains KSK-2010, but not KSK-2017
  - The dnssec-enable flag was set to false
  - The dnssec-validation flag was unset, leaving it in its default state of “yes.”



Resolver Telemetry: The return of KSK-2010



Discussion

VI

Do we need to improve telemetry?

- RFC 8145 and RFC 8509 are useful but should be improved
  - Allowing to identify the true source of a signal
  - Provide an estimate for how many users a signal represents

Photo by Chunlea Ju on Unsplash

Do we need to improve telemetry?

- RFC 8145 and RFC 8509 are useful but should be improved
  - Allowing to identify the true source of a signal
  - Provide an estimate for how many users a signal represents

Do we need to change trust anchor management?

E.g. shipping TAs centrally in OSes?

Photo by Chunlea Ju on Unsplash

Conclusions and broader Lessons

- The rollover was a **success**
- **Independent analysis** and measurements on the internet are valuable
- Telemetry must be kept in mind **at an early stage** of protocol development
- Trust anchors should be **managed centrally**

Conclusions and broader Lessons

- The rollover was a **success**
- **Independent analysis** and measurements on the internet are valuable
- Telemetry must be kept in mind **at an early stage** of protocol development
- Trust anchors should be **managed centrally**

Questions, suggestions, comments?

Data available at

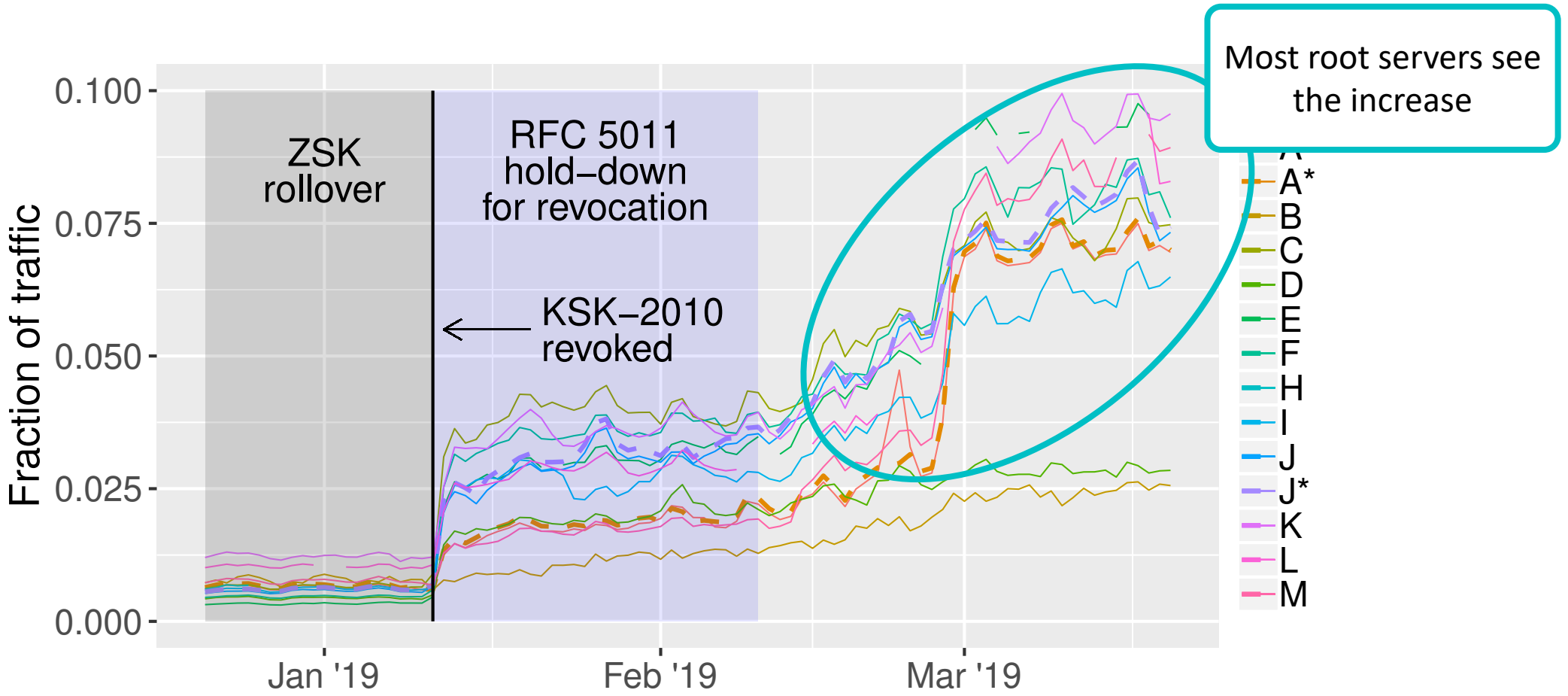
https://github.com/SIDN/RollRollRollYourRoot

Contact

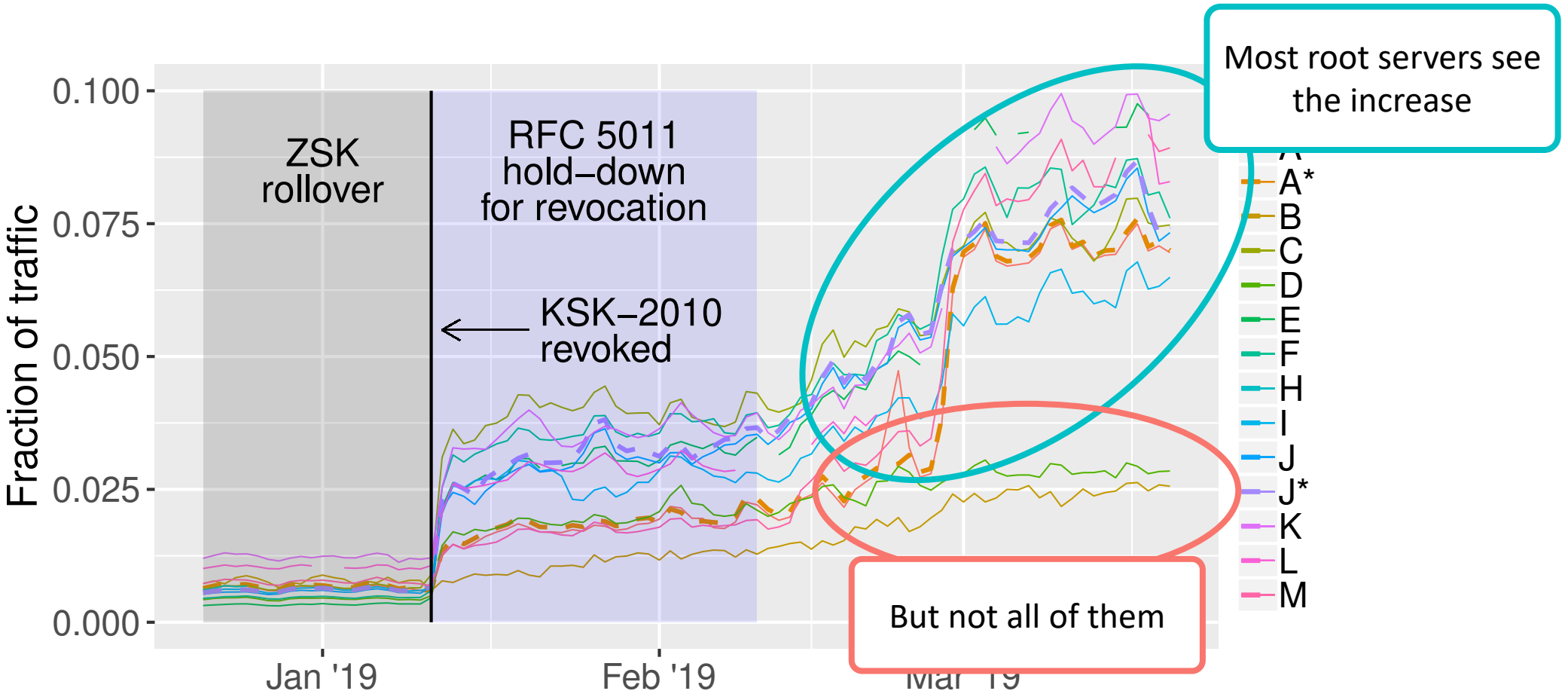
Moritz Müller | moritz.muller@sidn.nl | sidnlabs.nl

Bonus Slides

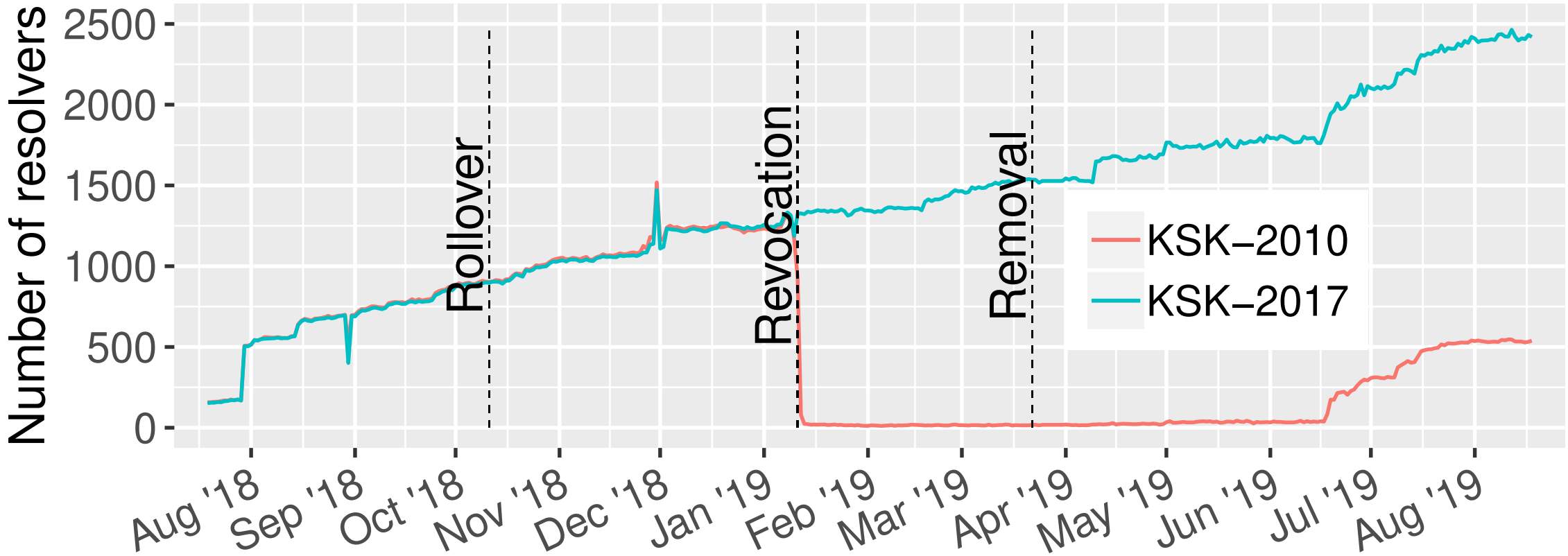
Increase in DNSKEY queries after revocation



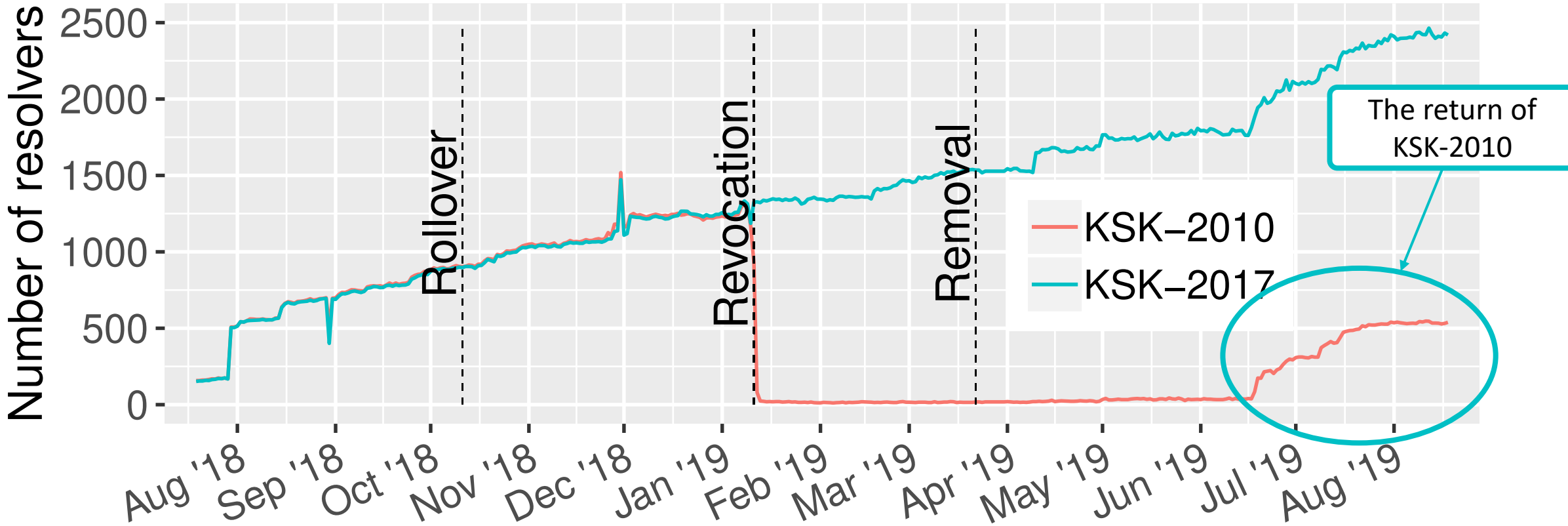
Increase in DNSKEY queries after revocation



Resolver Telemetry: RFC 8509 “Root Sentinel”

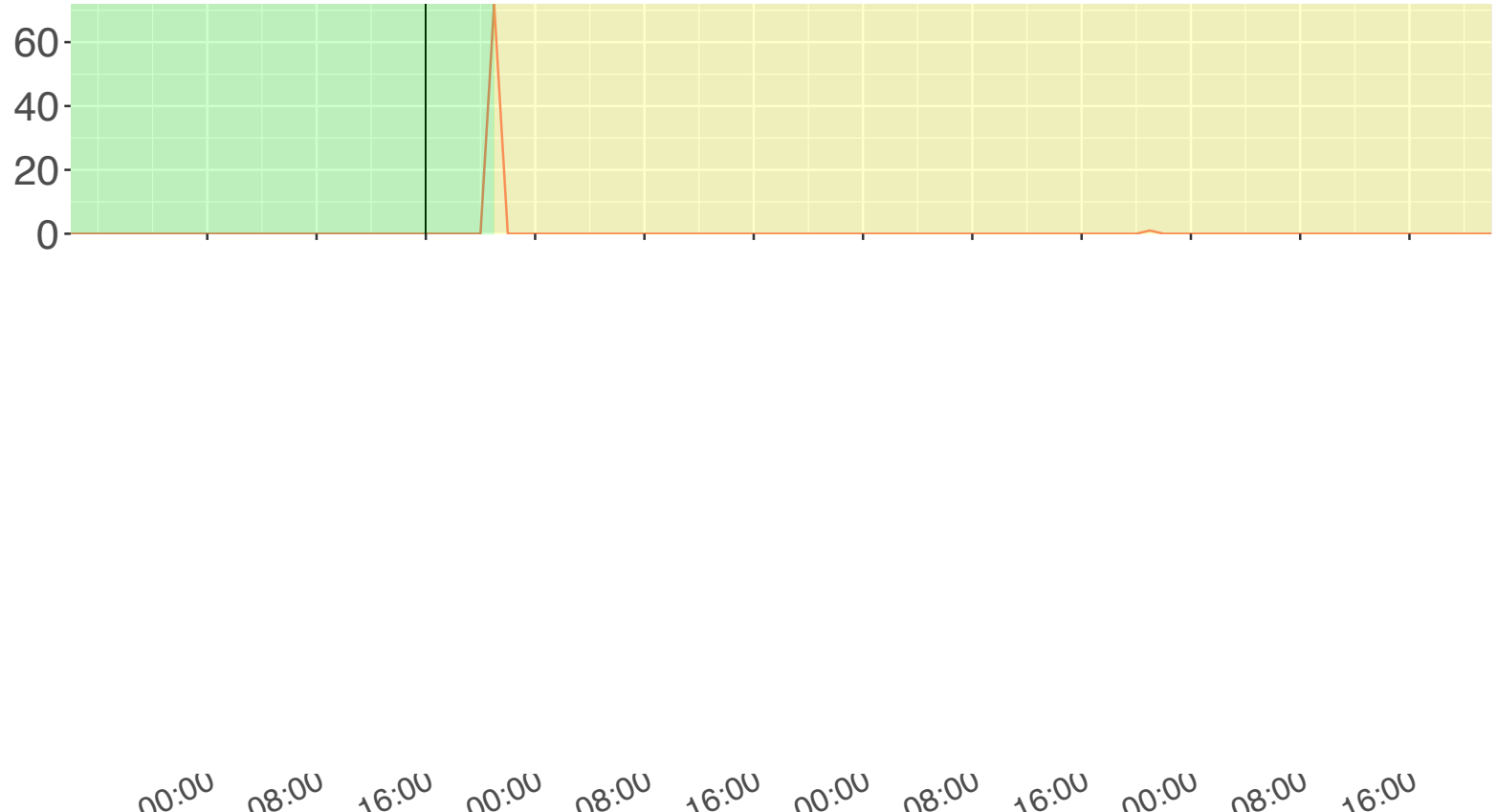


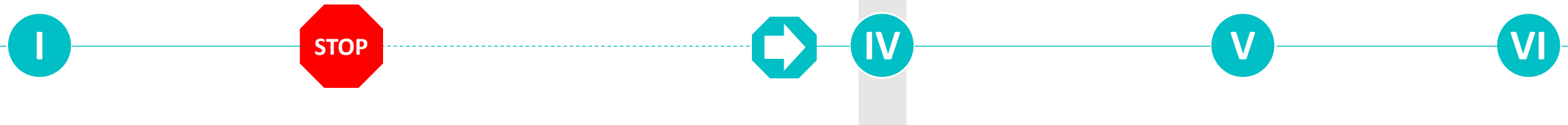
Resolver Telemetry: RFC 8509 “Root Sentinel”



Failure Modes

Failing and then Insecure

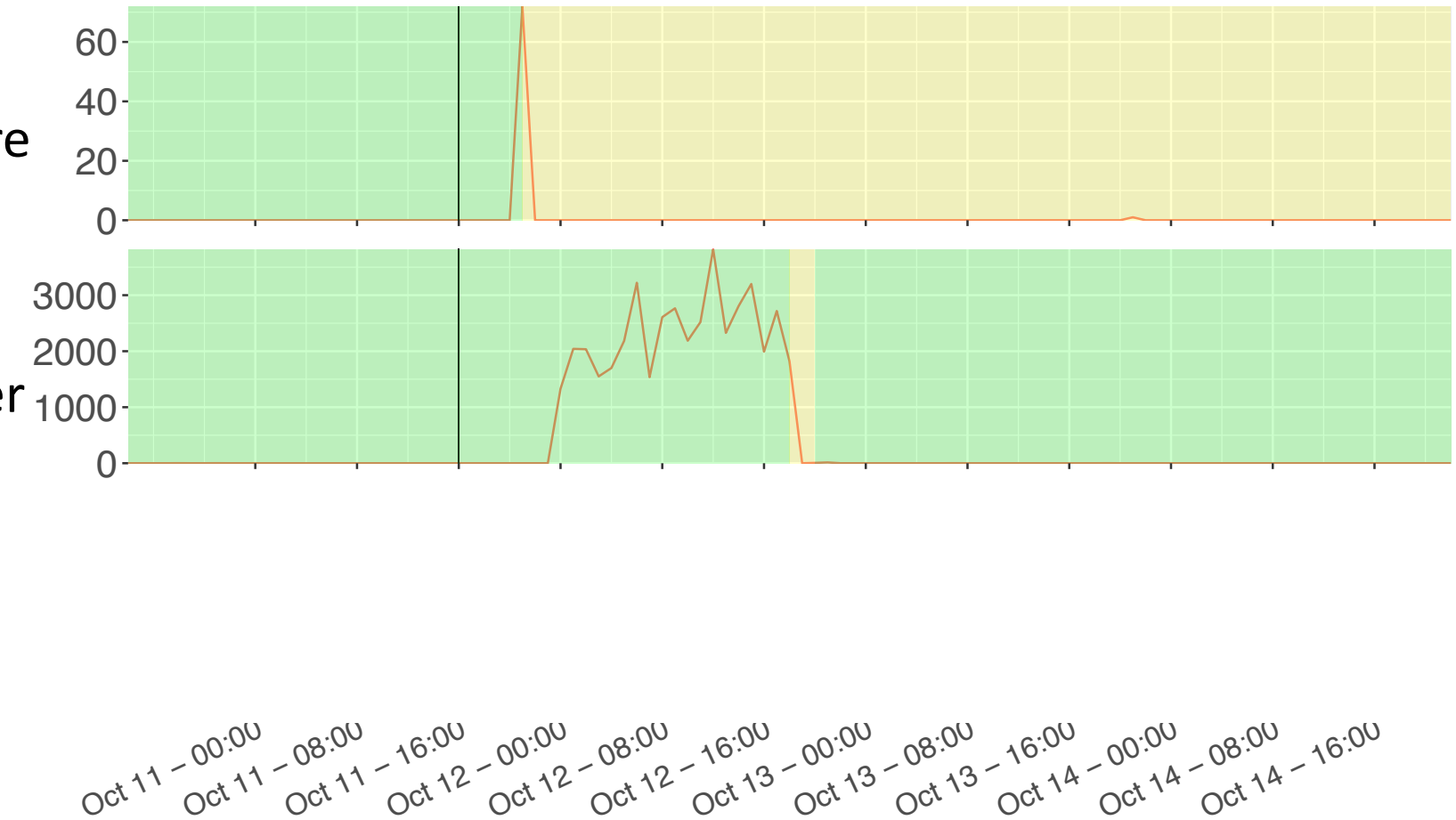




Validation Failure Modes

Failing and then Insecure

Failing and then Recover



Validation Failure Modes

Failing and then Insecure

Failing and then Recover

Failing and then Bogus