



Root Zone KSK Rollover

Matt Larson, VP of Research, Office of the CTO
matt.larson@icann.org | DNS-OARC 26 | May 14, 2017

Root zone KSK rollover

- ⦿ **There has been one root zone KSK**
 - ⦿ Since the root was first signed in 2010
 - ⦿ Called “KSK-2010”
- ⦿ **A new KSK will be used starting on 11 October 2017**
 - ⦿ An orderly succession for continued smooth operations
 - ⦿ Called “KSK-2017”
- ⦿ **Operators of DNSSEC validating resolvers may have some work**
 - ⦿ As little as review configurations
 - ⦿ As much as install KSK-2017

Root KSK rollover milestones

Event	Date
Creation of KSK-2017	27 October 2016
Operationally Ready	2 February 2017
Out-of-DNS-band Publication	Now (and onward)
In-band Publication	11 July 2017 (onward)
Sign the root key set (the actual rollover)	11 October 2017 (onward)
Revoke KSK-2010	11 January 2018
Remove KSK-2010 from ICANN facilities	Dates TBD, 2018

Measuring possible problems after the rollover

- ◉ ICANN Office of the CTO Research group working with Roland van Rijswijk, SURFnet/University of Twente
- ◉ Active measurement of rollover issues
- ◉ Thanks to Programme Committee for letting me yield time to Roland to describe his work



The Root Canary

measuring and monitoring the impact of the KSK rollover

UNIVERSITY OF TWENTE.



Canary in the coalmine



picture from academia.dk

Canary in the virtual coalmine

- Goals:
 - **Track operational impact** of the root KSK rollover, act as a warning signal that validating resolvers are failing to validate with the new key
 - **Measure validation during the KSK rollover** from a global perspective **to learn from this type of event**

Operational actions

- If the **canary** starts to sing, or keels over and **dies**: an **operator** of a validating resolver may be in **trouble!** This type of monitoring gives us **immediate insight** into **which operators have problems**
- **Notify** (large?) **operators** that they need to take action — while most likely all resolving will fail, it may not affect all of their resolvers, etc. etc.

Measurement goals

- This is the **first time** the root KSK is rolled
- Unique **opportunity** to record measurement data that can **provide insight into the impact** on the global Internet of such a rollover
- Goal is also to **establish an observatory** that covers the state of DNSSEC validation **from multiple angles**

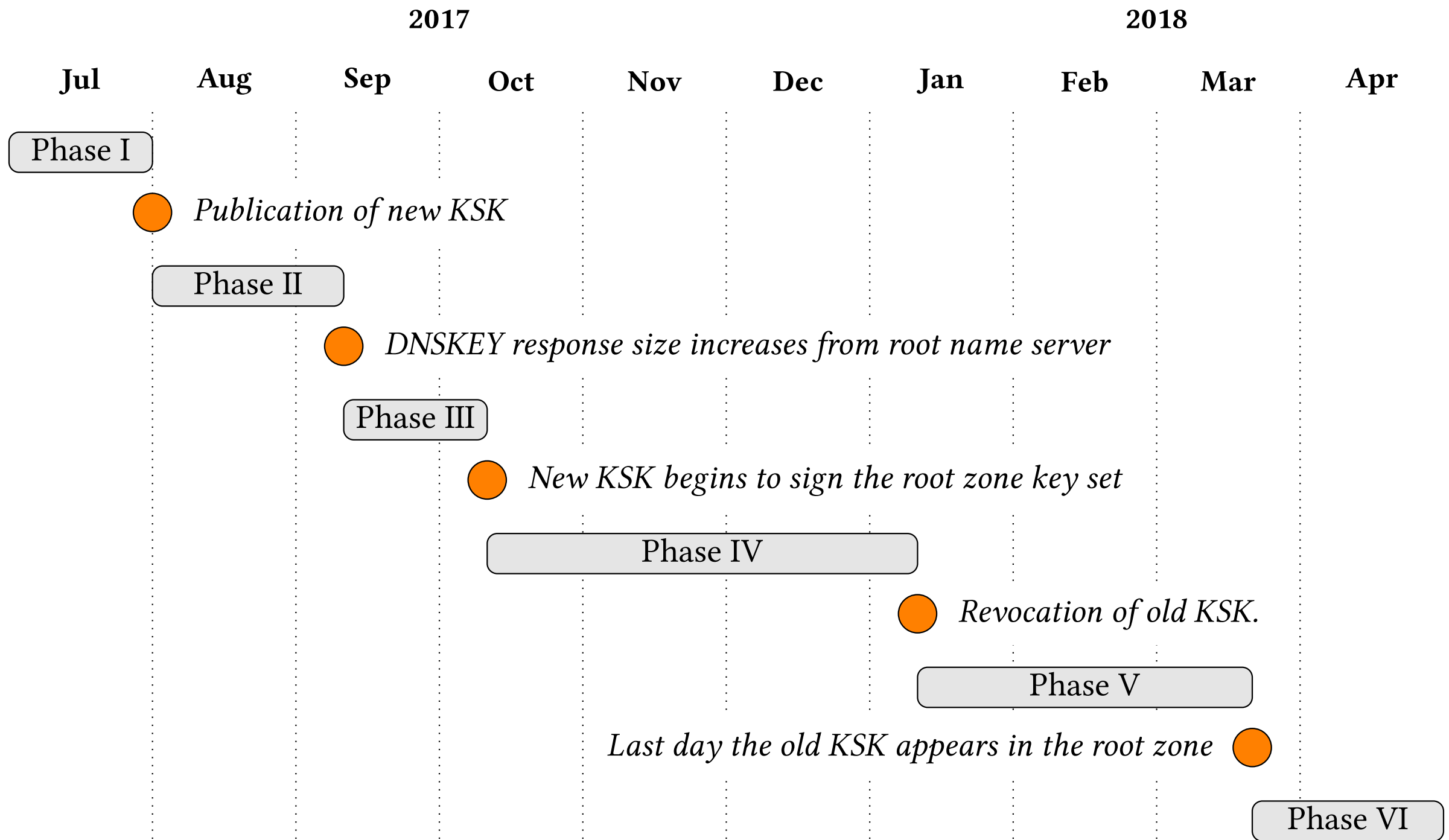
Measurement methodology

- Use four perspectives:
 - Online perspectives:
 - RIPE Atlas
 - Luminati
 - APNIC DNSSEC measurement
 - “Offline” perspective (analysed after measuring)
 - Traffic to root name servers (multiple letters)

Measurement methodology

- Plan is to have **signed and bogus** records for **all algorithms**
- **Side-effect:** measure support for algorithms
- This gives us one of four outcomes:
 - Resolver validates correctly
 - Resolver fails to validate (SERVFAIL)
 - Resolver does not validate
 - Yes, mr. Huston, there are corner cases probably not covered by the three options I originally had above ;-)

Measurement phases



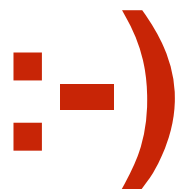
(picture courtesy of Taejoong “tijay” Chung, Northeastern University)

Coalition of the willing

- We have an informal coalition of partners working on this. All additional help is welcome!
- Current “coalition of the willing” (in alphabetical order):

ICANN
NLnet Labs
Northeastern University

RIPE NCC
SURFnet
University of Twente




Feedback welcome


- We have started designing our measurement infrastructure
- Your input is more than welcome! Any comments, suggestions, ..., please let us know.
- (Still) coming soon(-ish): **rootcanary.org**

Thank you for your attention!

Questions?

 nl.linkedin.com/in/rolandvanrijswijk

 @reseauxsansfil

 roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl



UNIVERSITY OF TWENTE.

