The Root Canary

measuring and monitoring the impact of the KSK rollover

Project partners

UNIVERSITY OF TWENTE.

SURF NET

Northeastern University

NLnet Labs

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ICANN

https://rootcanary.org/

Canary in the coalmine

picture from academia.dk

https://rootcanary.org/

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**

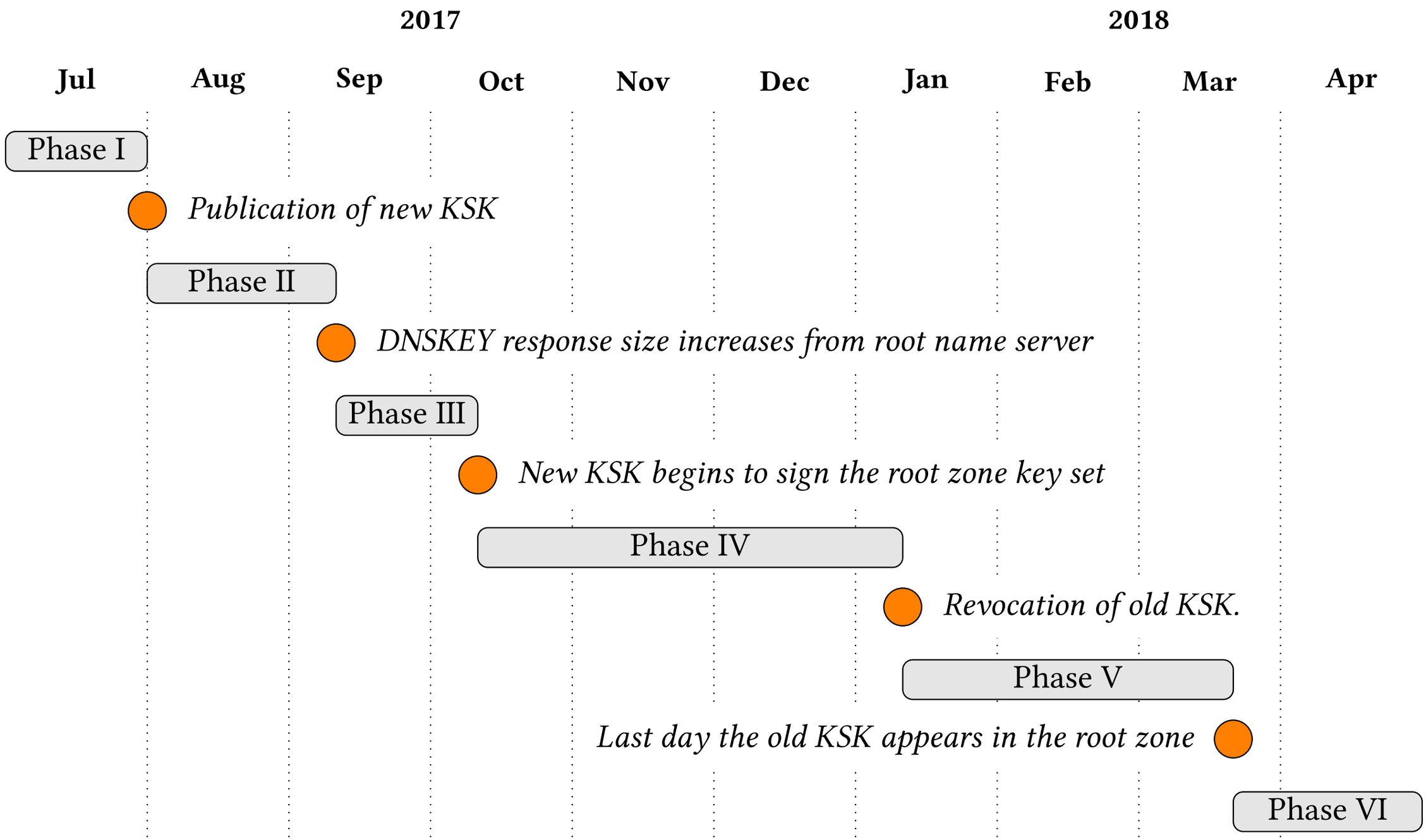
Measurement methodology

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

Measurement methodology

- We have **signed and bogus** records for **all algorithms** and **most DS algorithms**
- **Side-effect**: measure support for algorithms
- This gives us one of three outcomes:
  - Resolver **validates correctly**
  - Resolver **fails to validate** (SERVFAIL)
  - Resolver **does not validate**
  - (yes, there are **corner cases** probably **not covered** by these three options) ;-)

Measurement phases

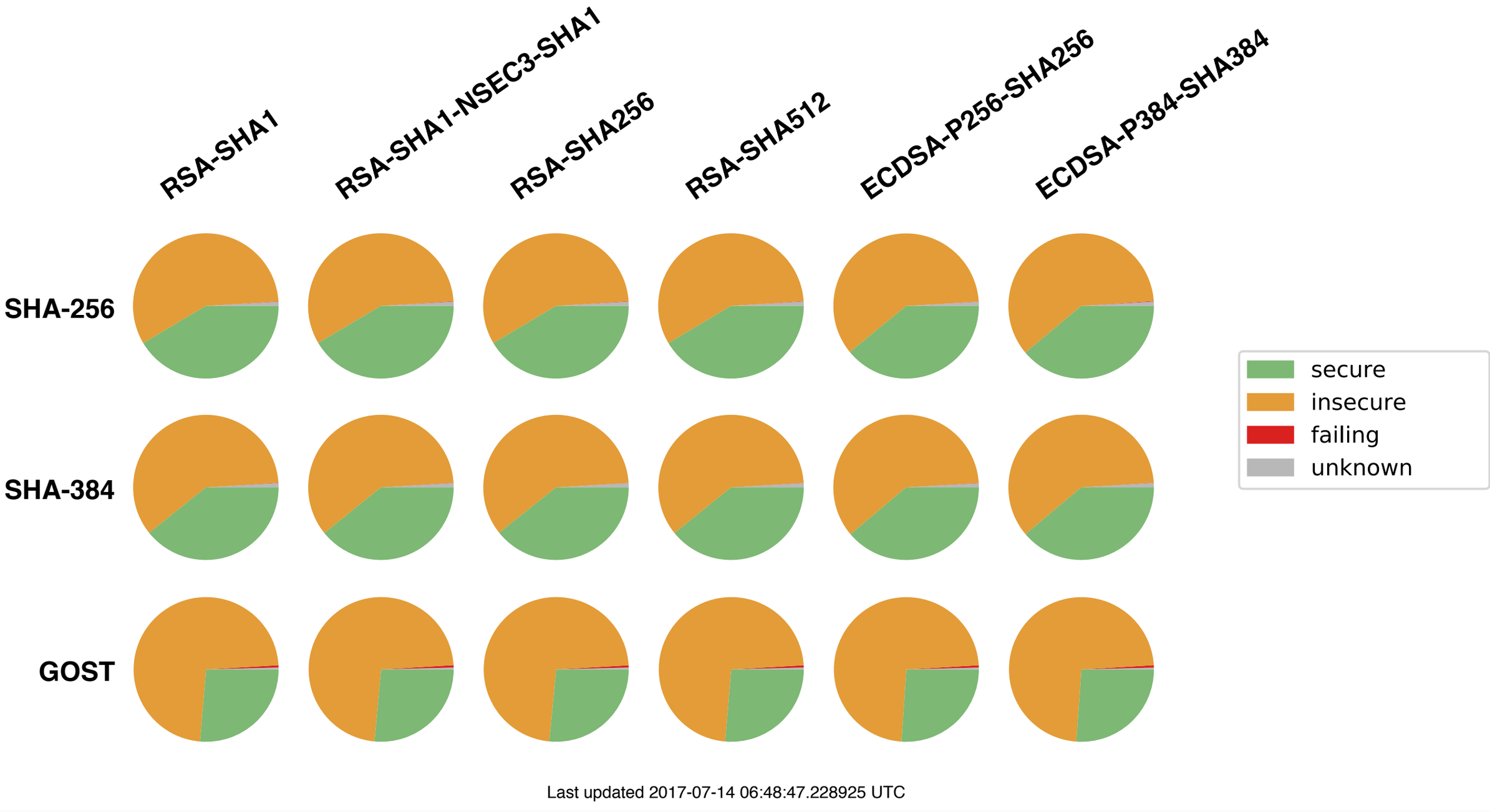


(picture courtesy of Taejoong “tijay” Chung, Northeastern University)

https://rootcanary.org/

First results

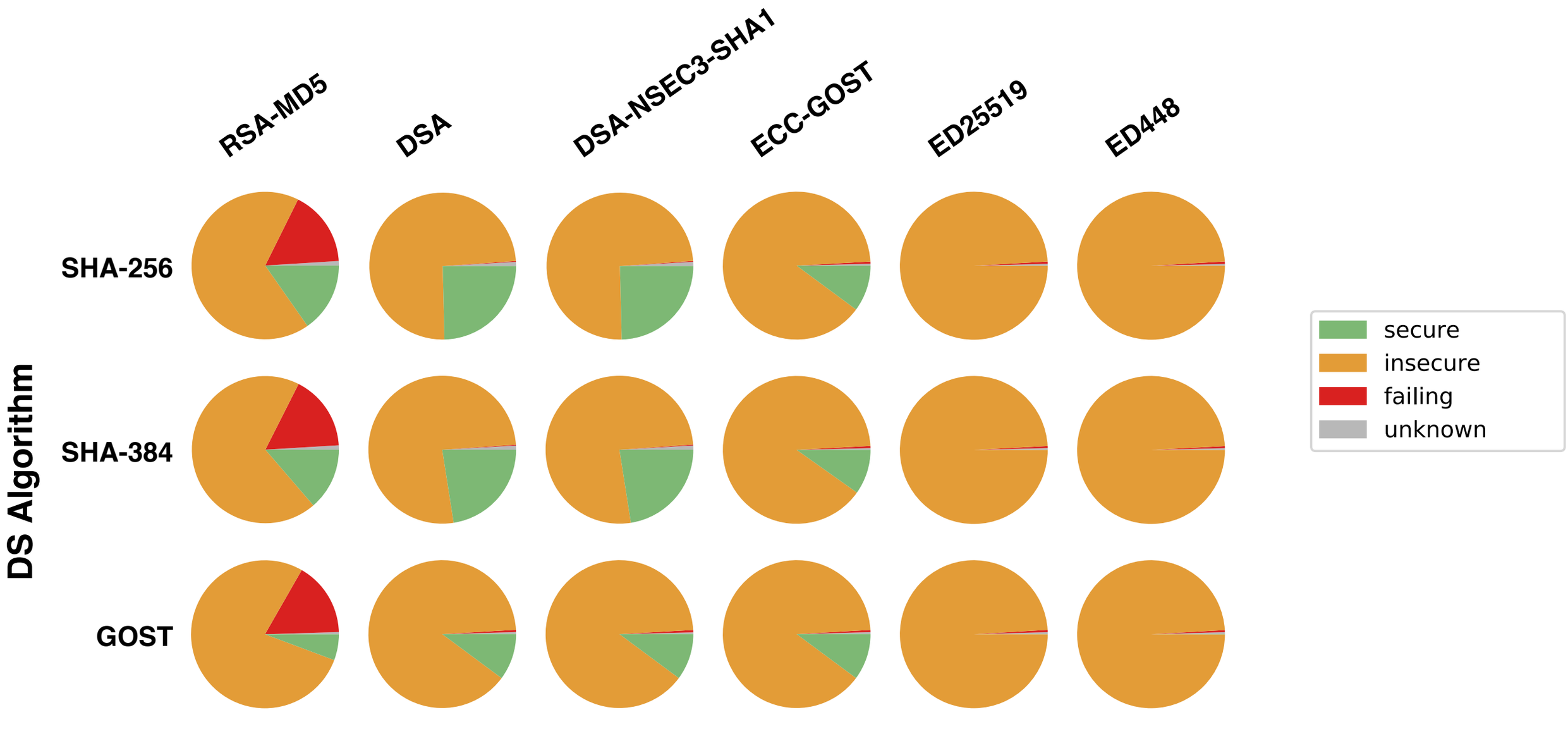
- For common signing algorithms:



https://rootcanary.org/

First results

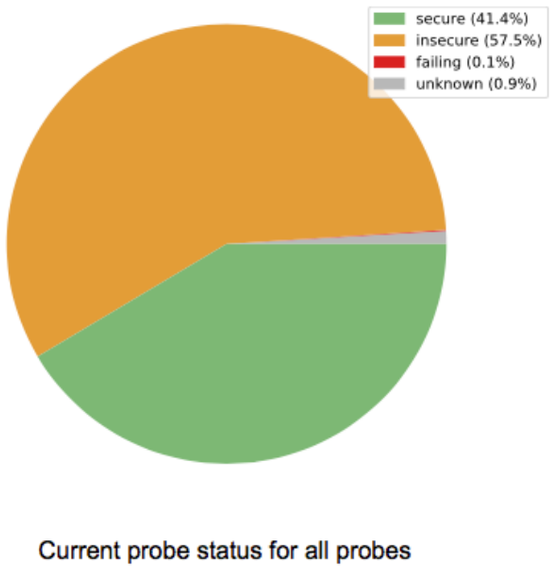
- For deprecated and brand new algorithms:



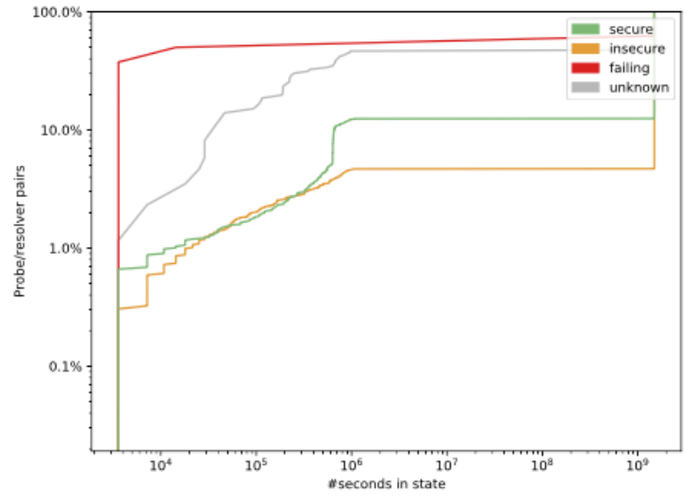
https://rootcanary.org/

First results (details)

current state of probe population

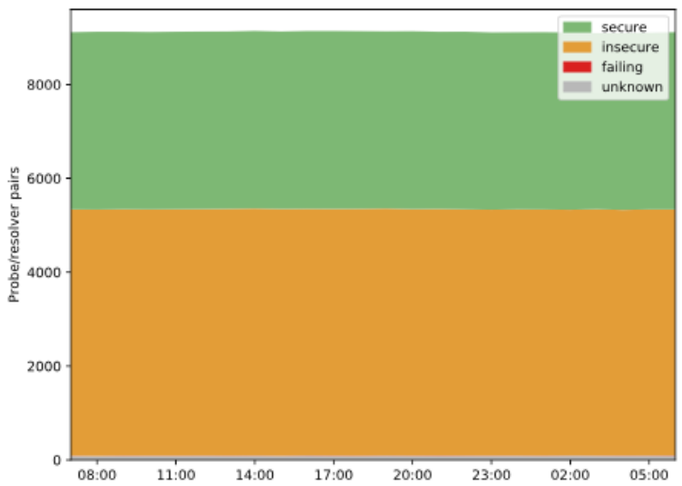


Current probe status for all probes

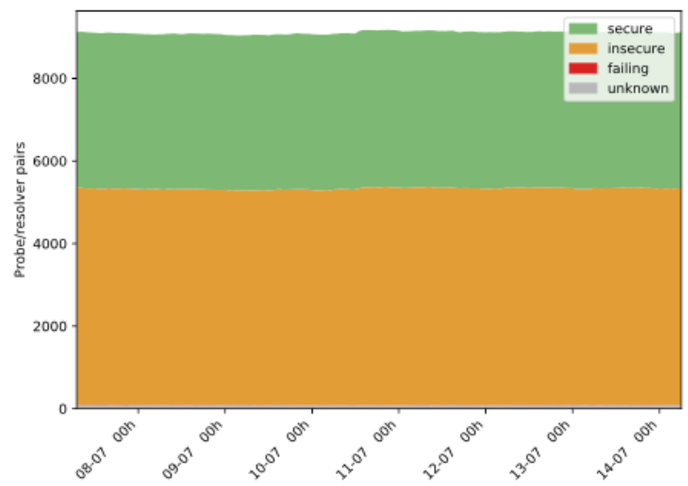


CDF for current time in state

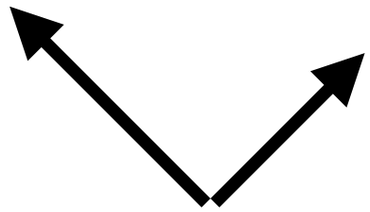
CDF for time probes are in a state (shorter == many state changes)



All probes (24h)



All probes (7 days)



total probe population state (24h and 7 days)

https://rootcanary.org/

Takeaways from first results

- **Introduction** of the **new key** on **July 11th** has **not led to** noticeable **problems** on resolvers

- Significant proportion of **RIPE Atlas probes** are **behind *stable* validating resolvers**

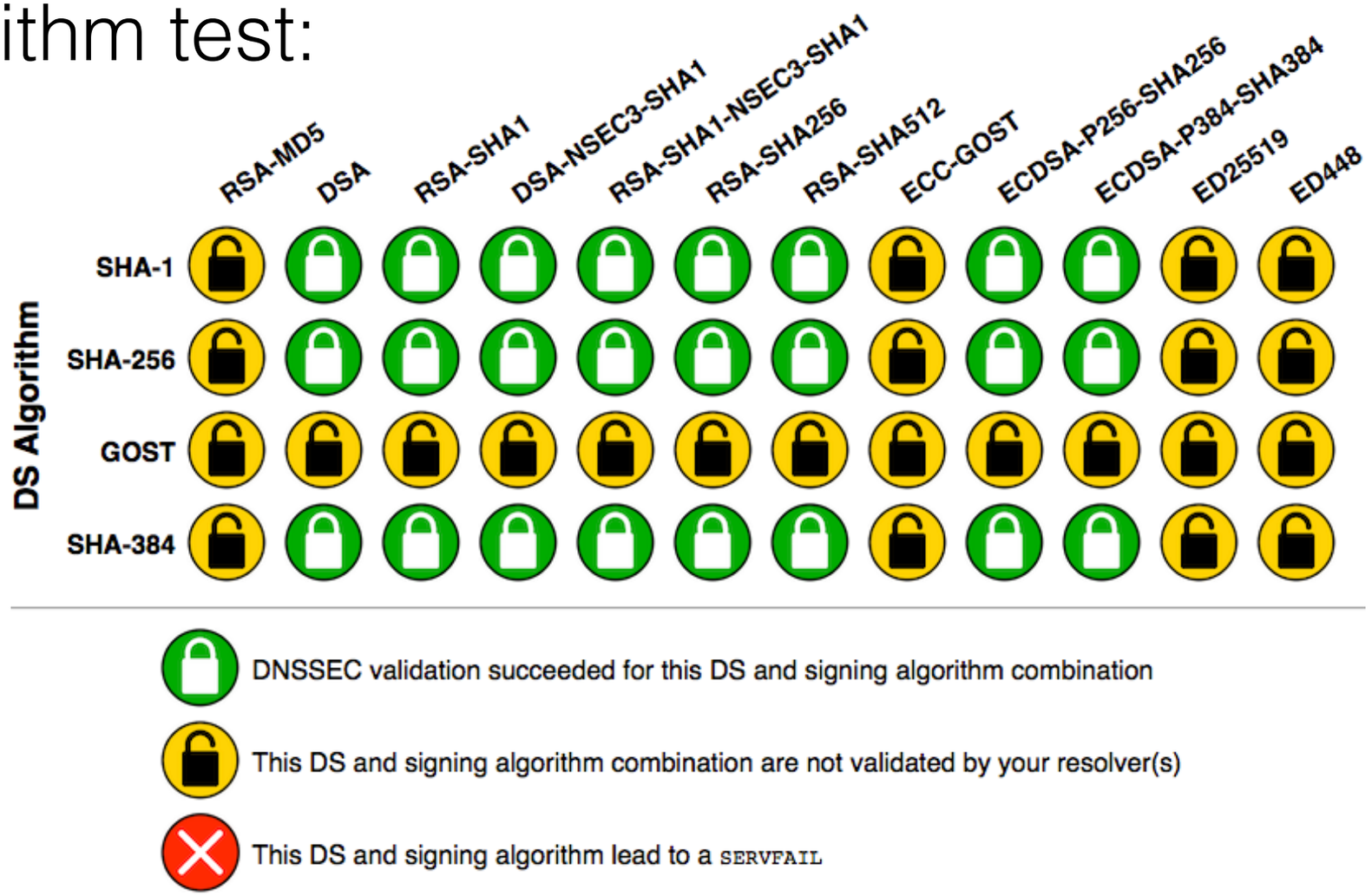
- **Google** Public DNS **returns SERVFAIL** for **RSA-MD5** (why not simply “insecure”?!)

- **Support** for **ECDSA P-256 and P-384** almost **at** the **same level** as support for **RSA-SHA256**

- Support for **Ed25519** and **Ed448** is **non-existent**

Spin-off result

- Some of you may have already seen our DNSSEC algorithm test:



- Online test checks DS- and signing algorithms supported by configured resolvers

https://rootcanary.org/

Spin-off result

- Algorithm **test** has **already led to fixes** in:
  - **PowerDNS** —> test showed it returned SERVFAIL for domains signed using algorithms it didn't support, and faulty Ed25519 signatures
  - **Knot Resolver** —> test also showed SERVFAIL returns for unsupported algorithms [1]

[1] https://gitlab.labs.nic.cz/knot/knot-resolver/issues/210

Work in progress

- Live feed of state changes for observed resolvers
- Portal environment that shows measurement state for DNS resolvers covered by RIPE Atlas probes
- Next upcoming major change: **size of DNSKEY response for the root grows on September 19th**
- …

https://rootcanary.org/

More info

- Project webpage:
  https://rootcanary.org/

- Online algorithm test:
  https://rootcanary.org/test.html

- Current results for RIPE Atlas-based measurement:
  https://portal.rootcanary.org/rcmstats.html