

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

Roland van Rijswijk-Deij^{*,☆}
r.m.vanrijswijk@utwente.nl

Taejoong Chung^{*}
David Choffnes^{*}
Alan Mislove^{*}

Willem Toorop[‡]

[★] Design and Analysis of Communication Systems (DACs),
Faculty of Electrical Engineering, Mathematics and Computer Science,
University of Twente, Enschede, The Netherlands
[☆] SURFnet bv, Utrecht, The Netherlands
^{*} Northeastern University, Boston, MA, United States
[‡] NLnet Labs, Amsterdam, The Netherlands

What?

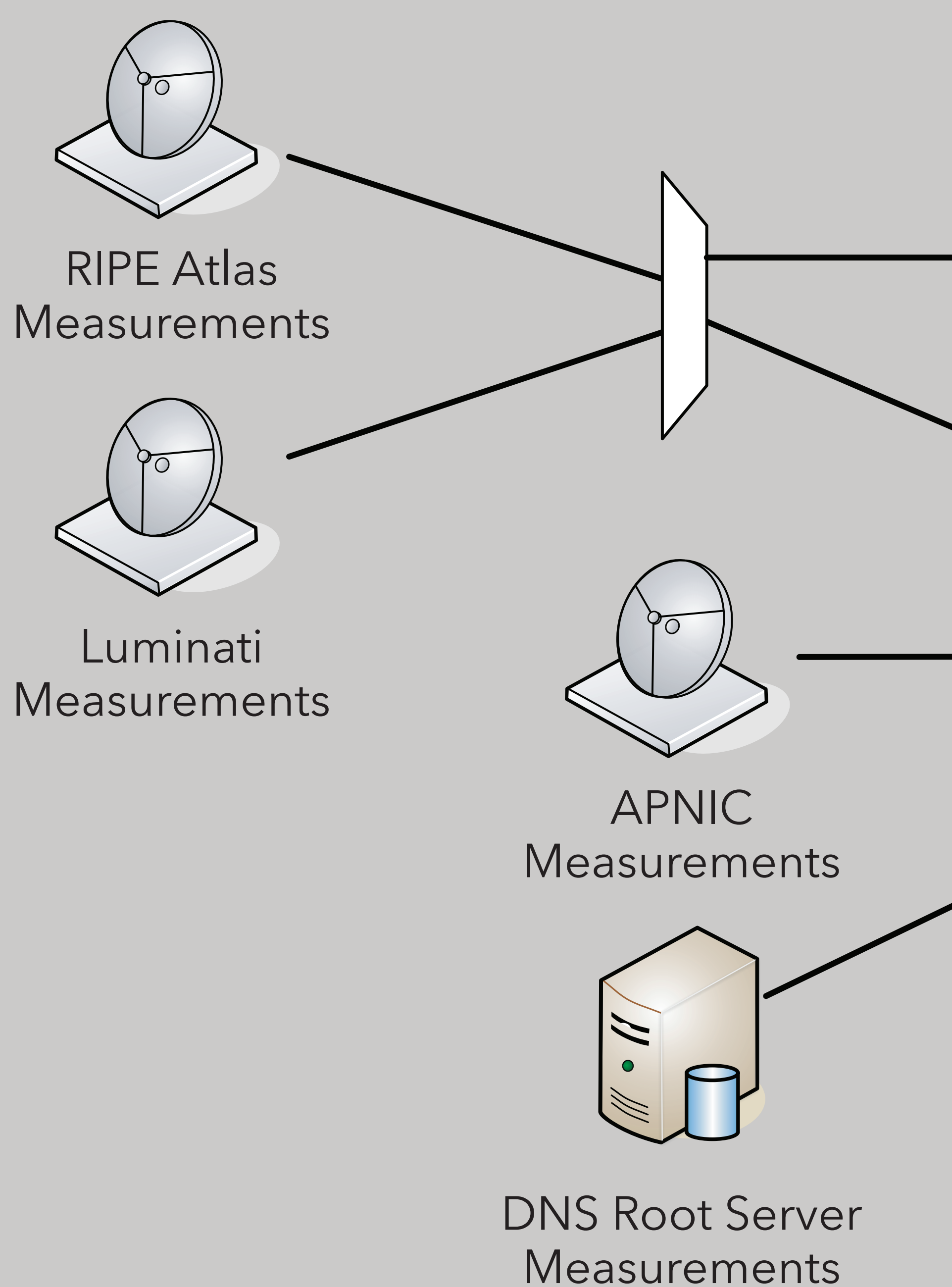
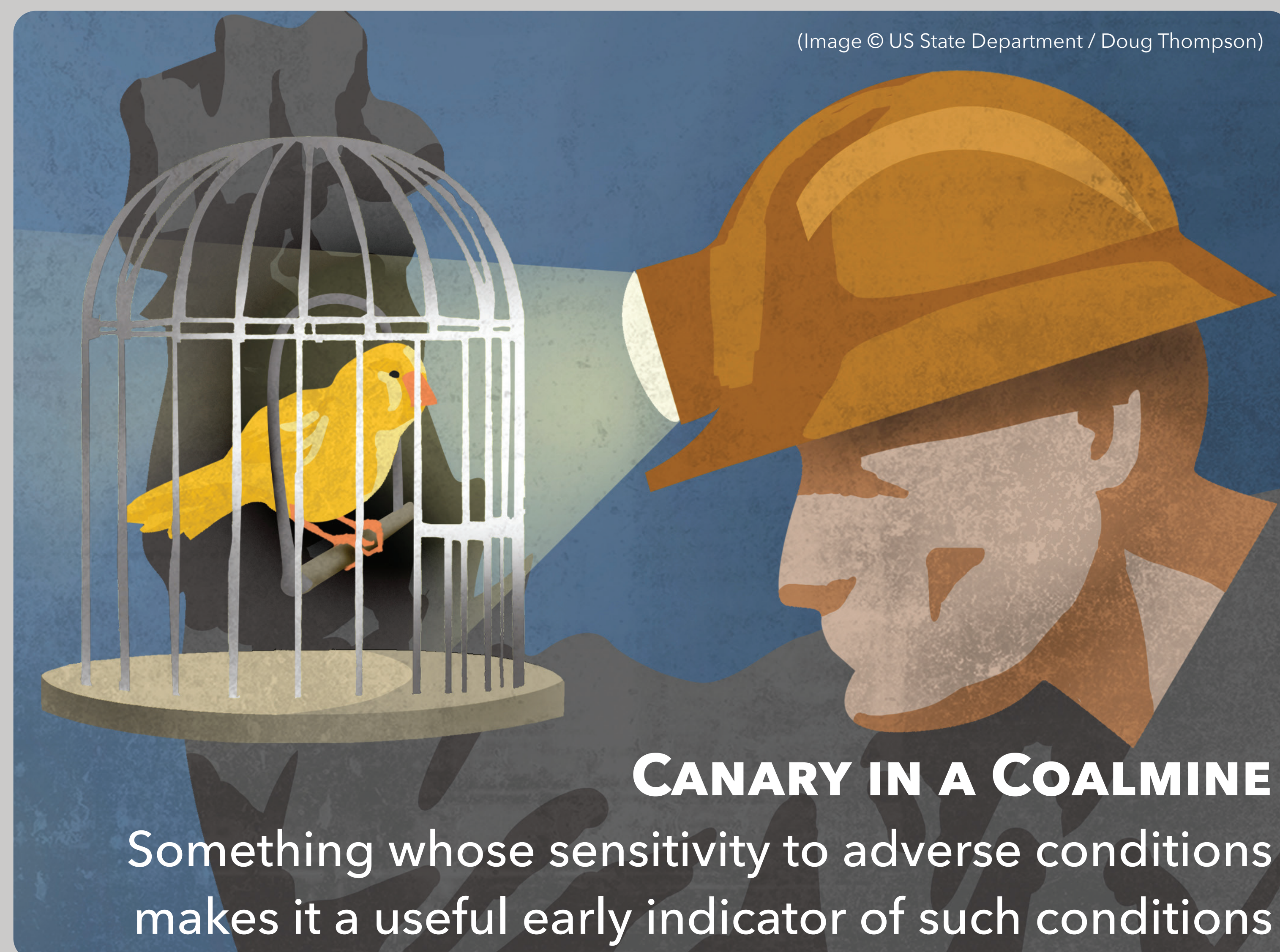
DNSSEC turns the DNS into a **Public Key Infrastructure**, where the root of trust is the so-called **Key Signing Key (KSK)** for the **root of the DNS**. This year, **for the first time ever**, this key will be replaced in a so-called **key rollover**.

Why?

This **unique event** can have significant **operational impact on the Internet**. Thousands of **validating DNS resolvers** serving **tens of millions of Internet users** **rely on this key** to validate DNSSEC signatures. These **resolvers** must **pick up the new key** through **automated or manual** processes. **Failure to pick up the new key** can lead these **resolvers** to become **inoperative**.

How?

We **combine** (figure below) four sources of **active** and **passive measurements** to get **maximum visibility** of the DNS resolver ecosystem. Using this data we perform **near real-time monitoring** during the entire rollover process (figure below right) and will **analyse the impact of the rollover** after the process completes.

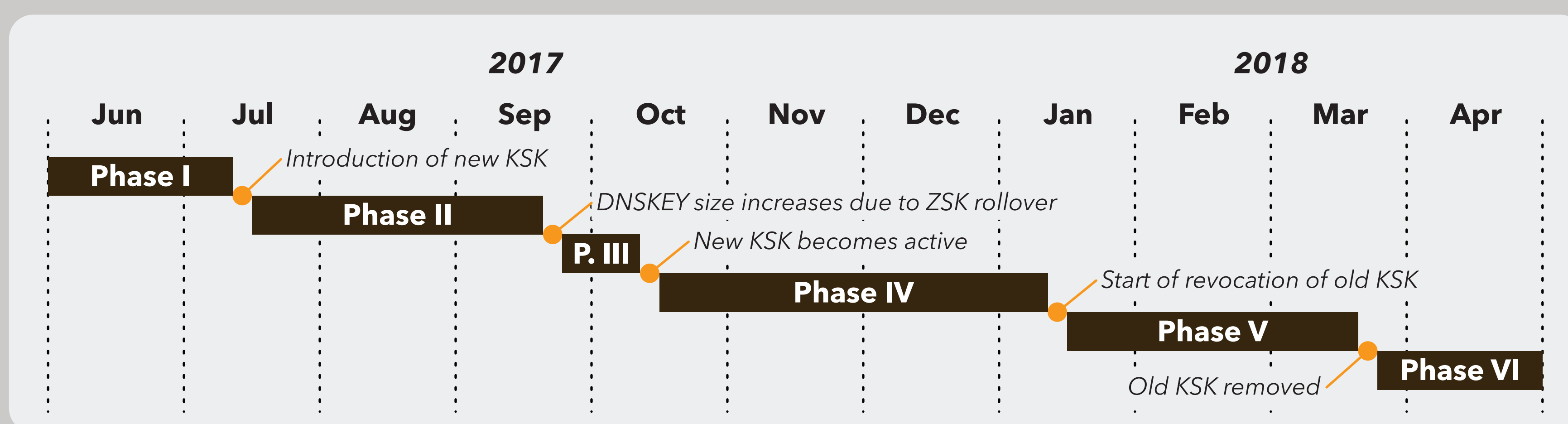


Near real-time monitoring

- Web portal
- Live feed with resolver status events
- Actionable data to support operational decisions during the KSK rollover process

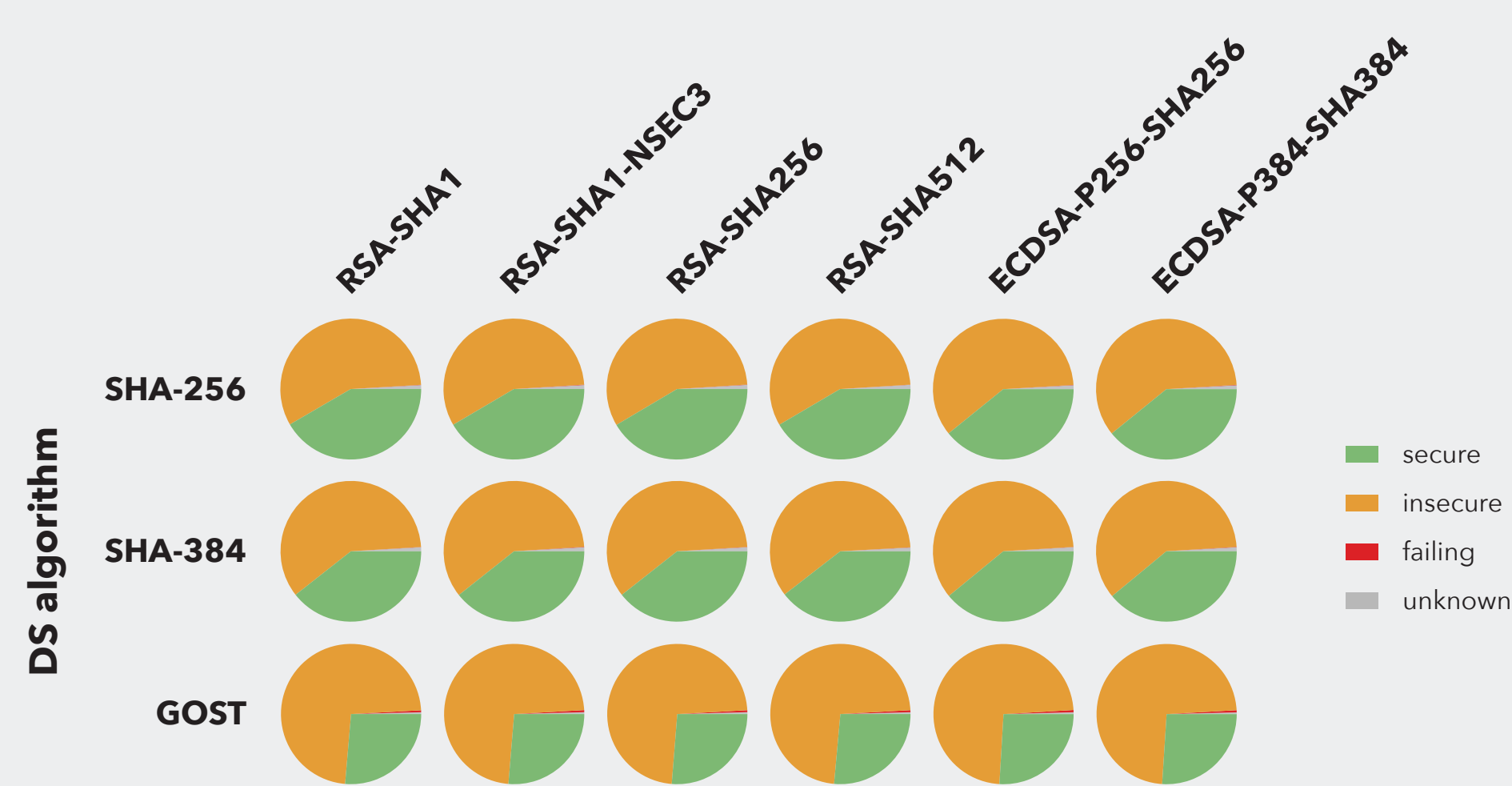
Analysis of full rollover process

- After KSK rollover completes in March '18
- Learn from problems
- Inform policy for future root KSK rollovers



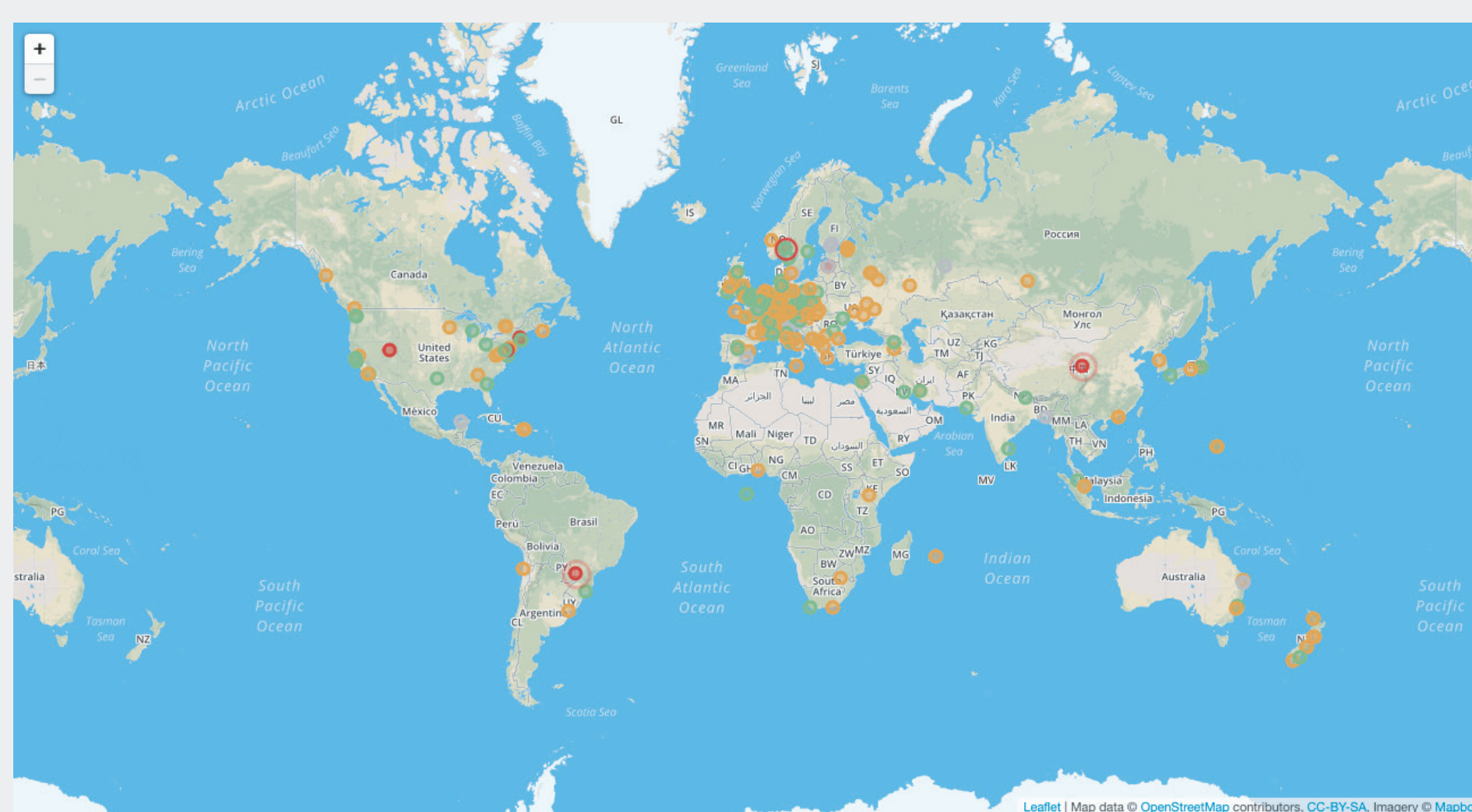
Preliminary Results

Support for DNSSEC signing algorithms



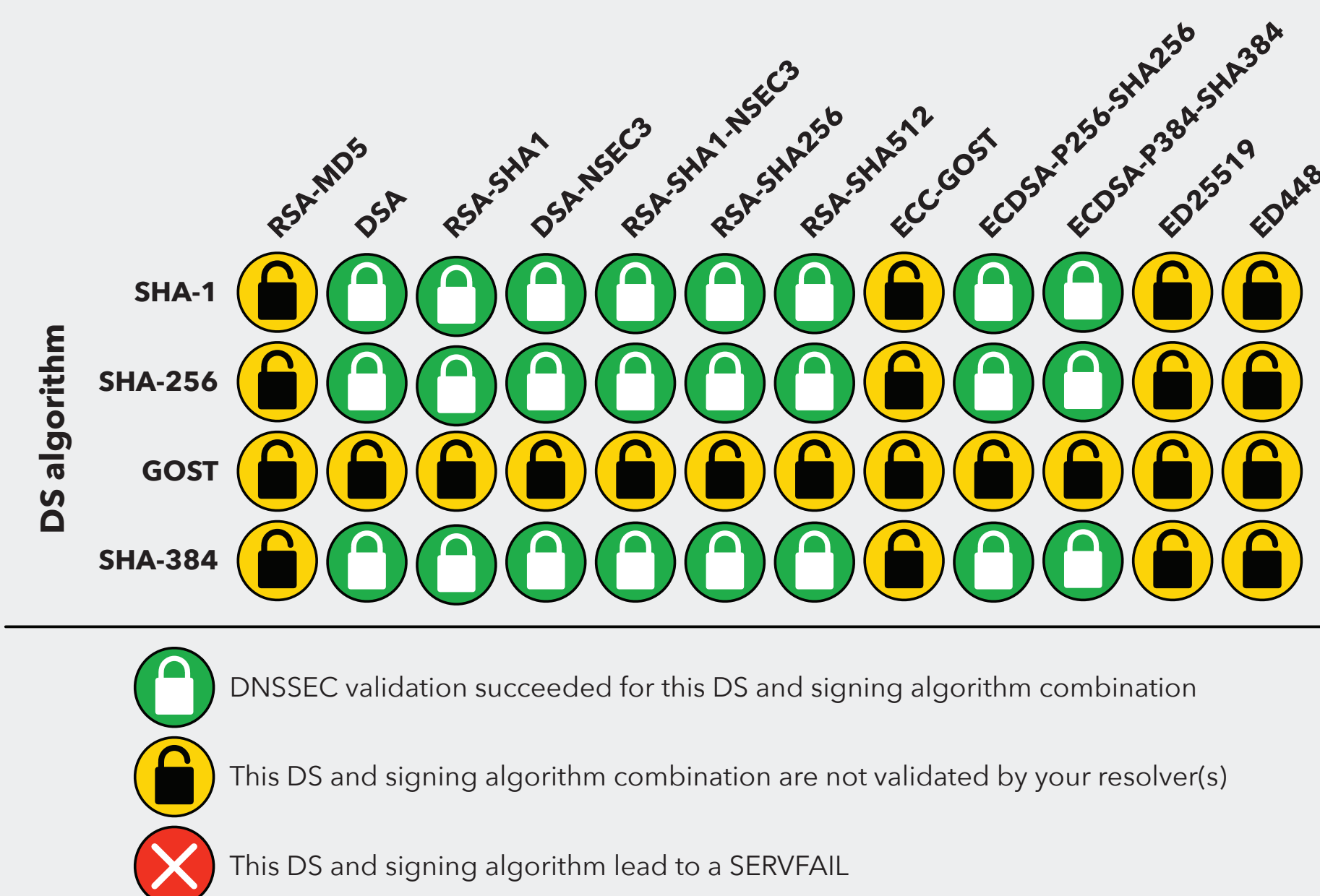
portal.rootcanary.org/rcmstats.html

Live probe status reports



monitor.rootcanary.org/live.html

Online algorithm support test



rootcanary.org/test.html