

# Rolling with Confidence

## Managing the Complexity of DNSSEC Operations

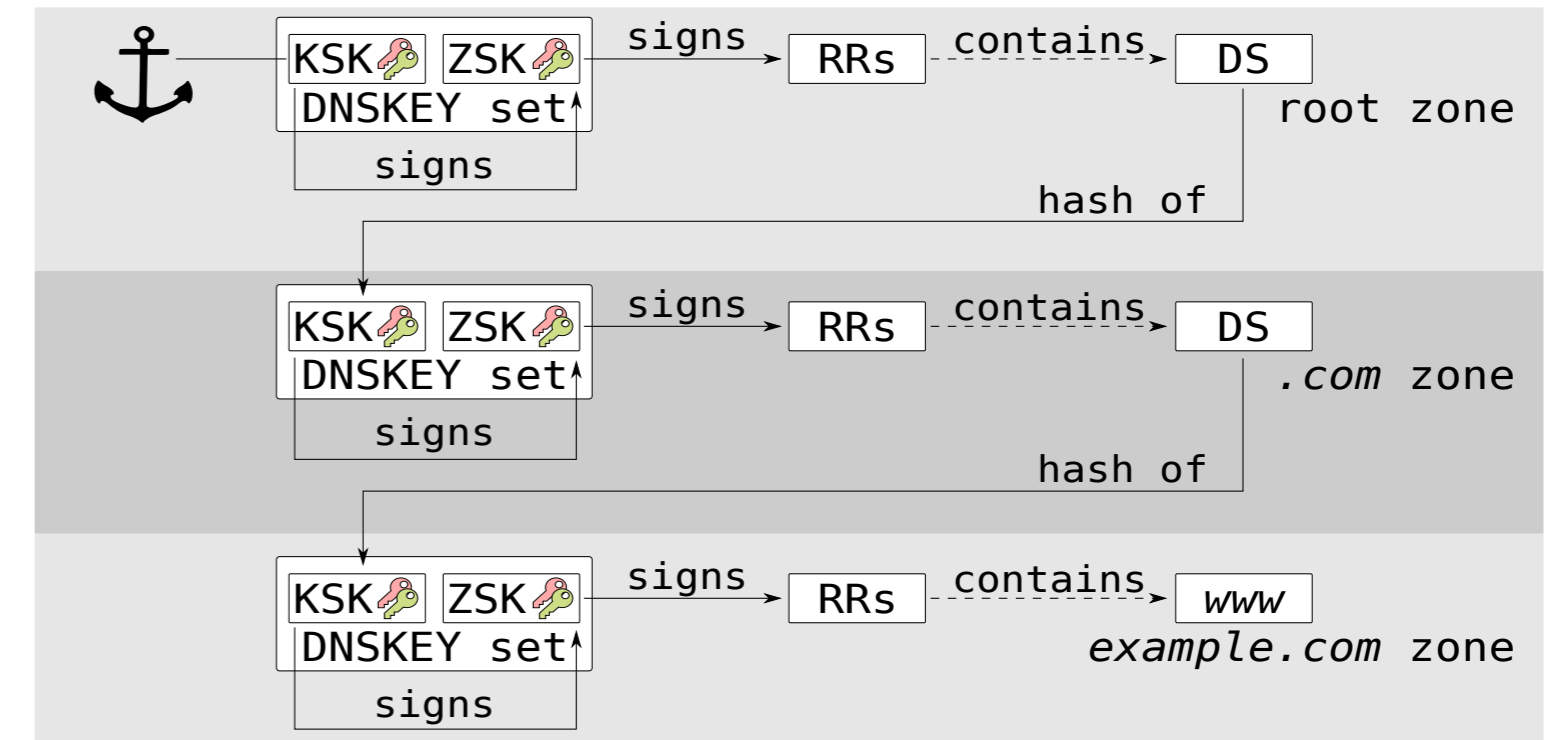
Extended Abstract

Moritz Müller  
moritz.muller@sidn.nl

Taejoong Chung  
t.chung@northeastern.edu

Roland van Rijswijk-Deij  
r.m.vanrijswijk@utwente.nl

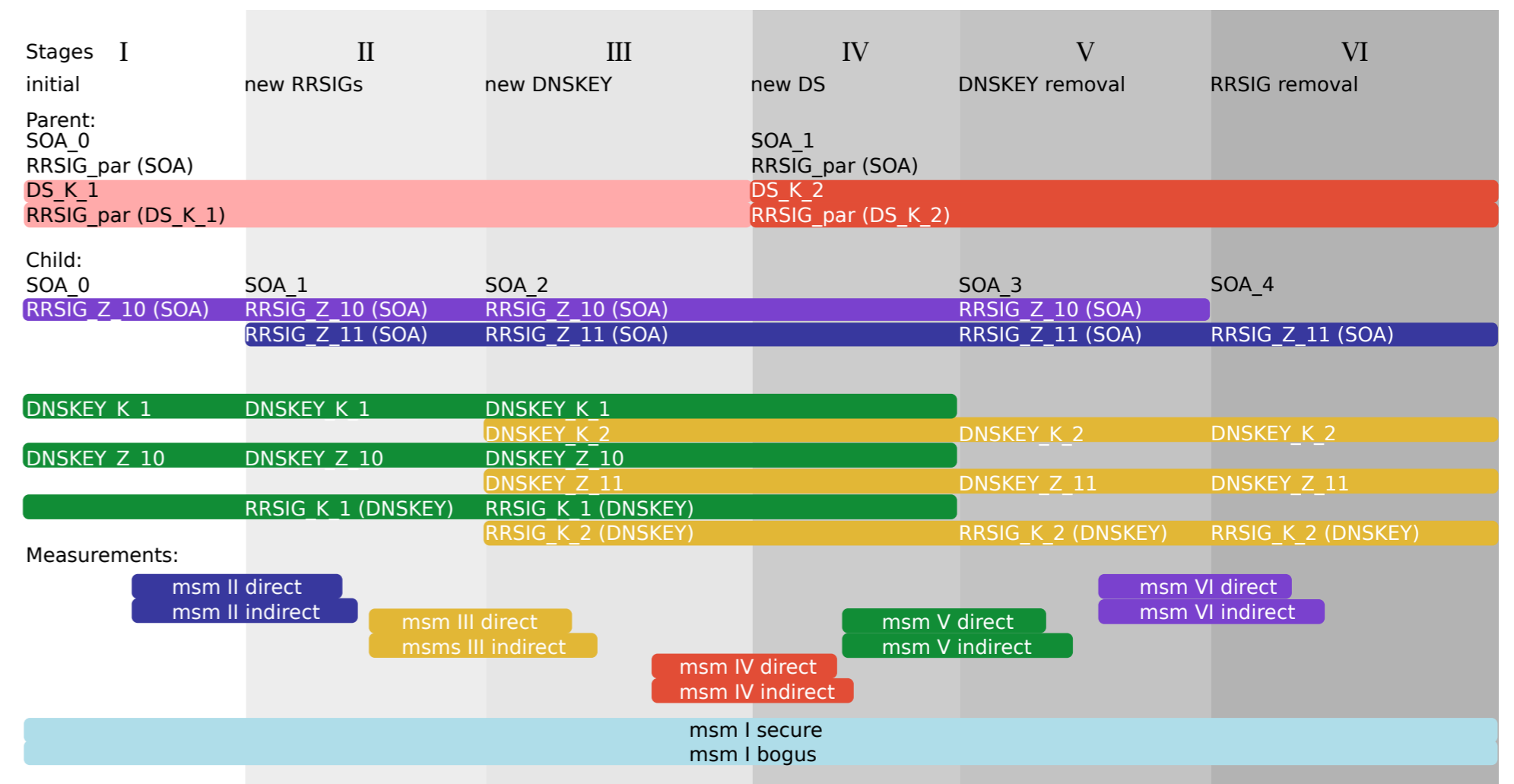
- DNSSEC secures the DNS, using public-key cryptography (PKI)
- DNS operators need to roll their keys (KSK or ZSK), in case of a:
  - key compromise
  - key management policy
  - algorithm change
- Errors during a rollover can have a massive impact on the availability of a domain



The DNSSEC chain of trust

### ⌚ Right timing is crucial

- DNS recursive resolvers cache records
- Keys withdrawn too early can lead to validation errors
- DNSSEC keys need to be rolled in stages
- It is safe to move to the next stage after:
  - every name server serves the new records (publication delay)
  - and every resolver has the new records in cache (propagation delay)



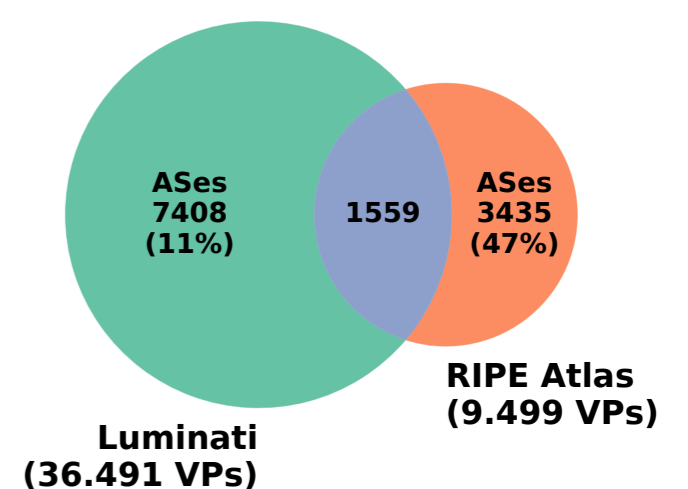
Algorithm rollover stages according to RFC6781

The methodology lets operators define the correct timing

### 📊 How to monitor a DNSSEC algorithm rollover - the .se use case

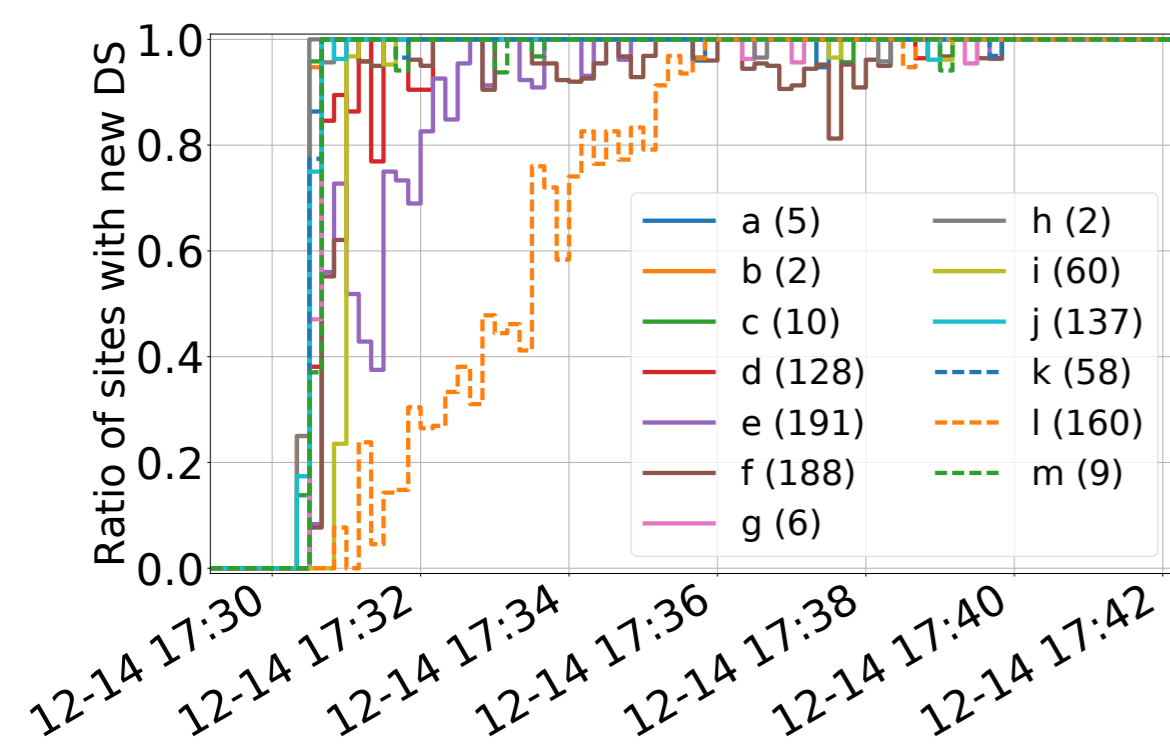
- We monitor the algorithm rollover of the Swedish ccTLD .se
- Any error would make 1.4 M domains unavailable
- At each stage: Monitor the propagation and publication delay, and the trust chain to validate the deployment

- Using RIPE Atlas and Luminati
- >46.000 vantage points (VPs)

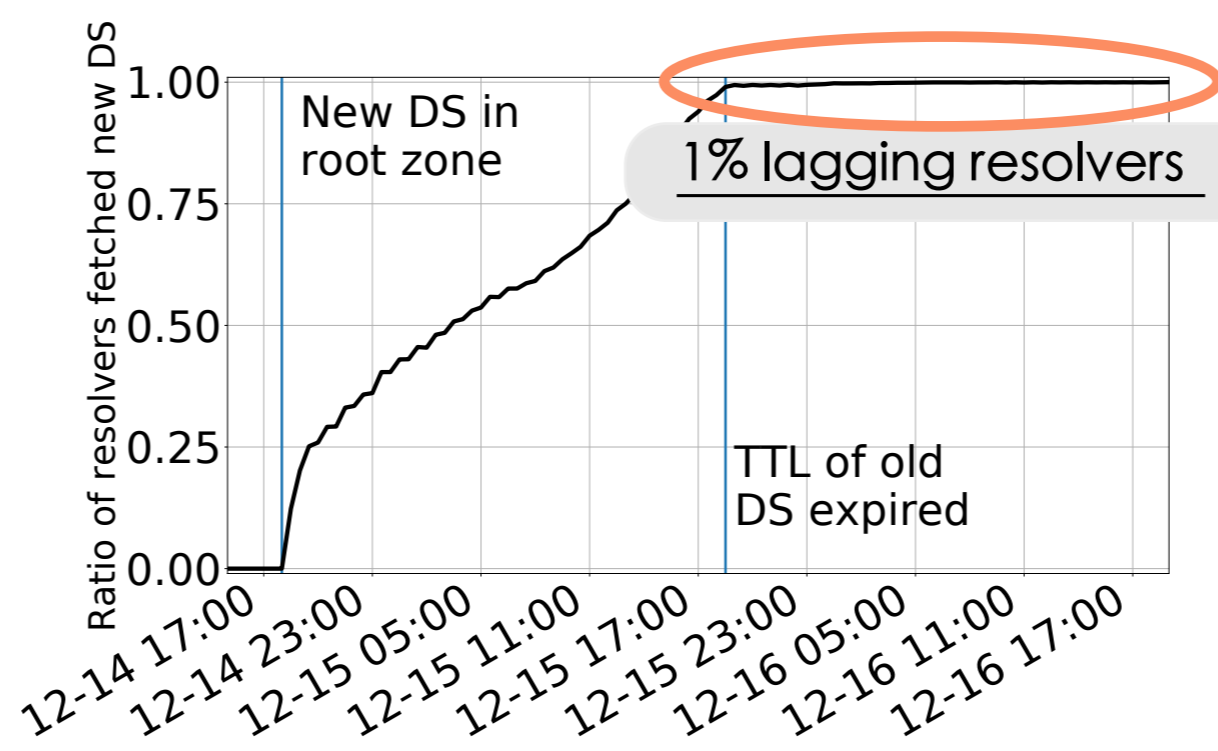


Example: Stage IV - Replacing the DS at the root

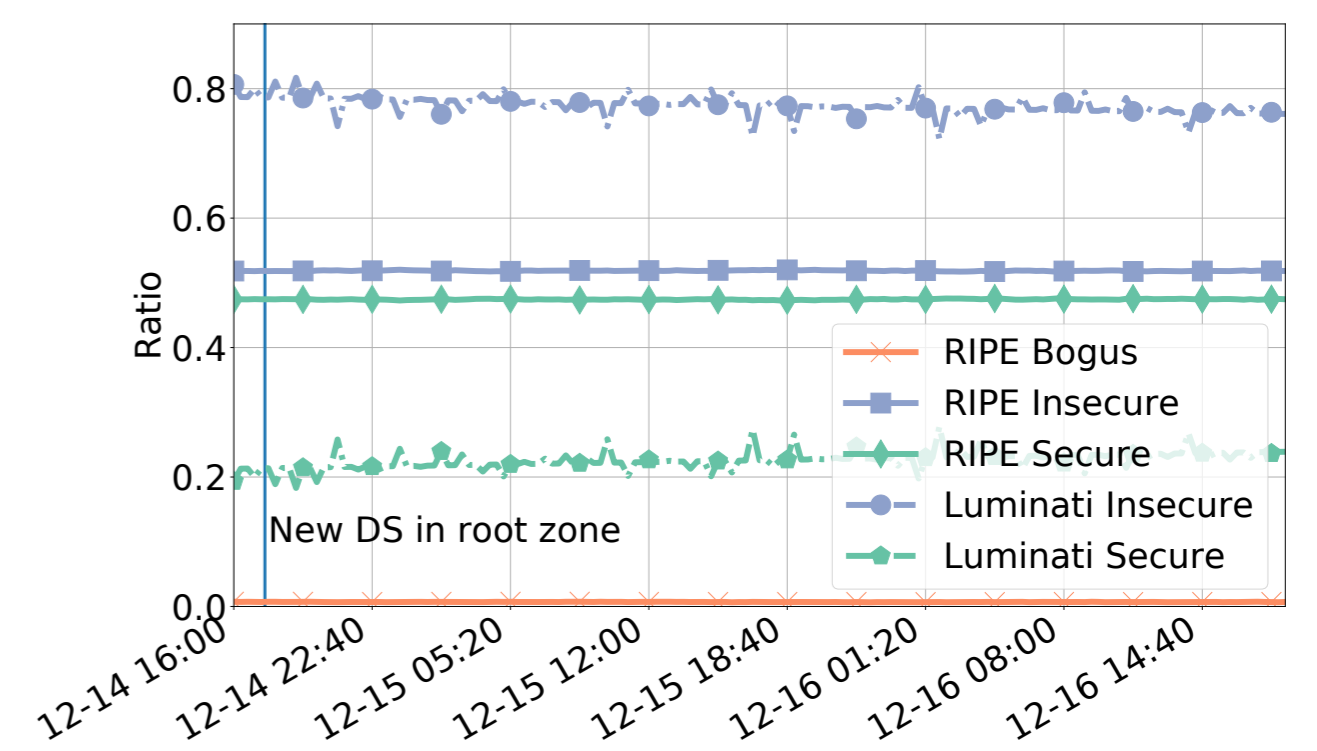
#### Publication Delay



#### Propagation Delay



#### Trust Chain



- Delay at the root servers 10 minutes
- Delay at some VPs 24h longer than expected
- No validation errors during the rollover

 **.se Rollover was a success!**

- We will make the measurement methodology and measurement tool available
- We also monitor the, even more critical, KSK rollover of the root: rootcanary.org



Read our blog post for more details:  
<http://bit.ly/2tsCjbm>



UNIVERSITY OF TWENTE.



Northeastern