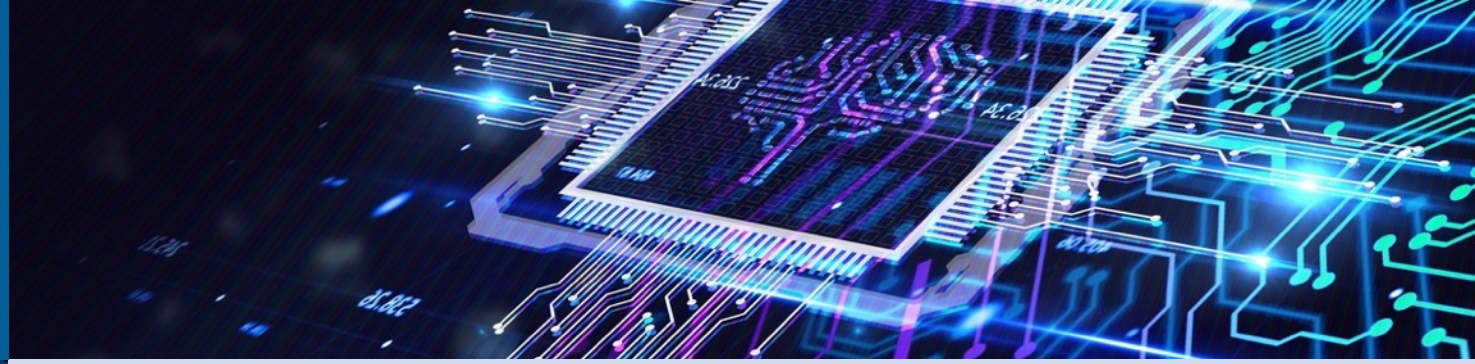
CSC

ICT Solutions for Brilliant Minds



DNSSEC algorithm rollover at .FI

nog.fi 2025.06
Juha Suhonen / CSC

DNSSEC in .fi

- .fi has been DNSSEC signed from 2010
  - Alg 8 and NSEC3 with salt + 5 iterations
- There are 550 000 .fi domains, but only 5 % have DS records

- TRAFICOM wanted to change to Alg 13 and NSEC3 with no salt + no iterations
  - Primary motivator: Reduce amount of TCP DNS query traffic
  - Secondary motivator: Follow current best practices

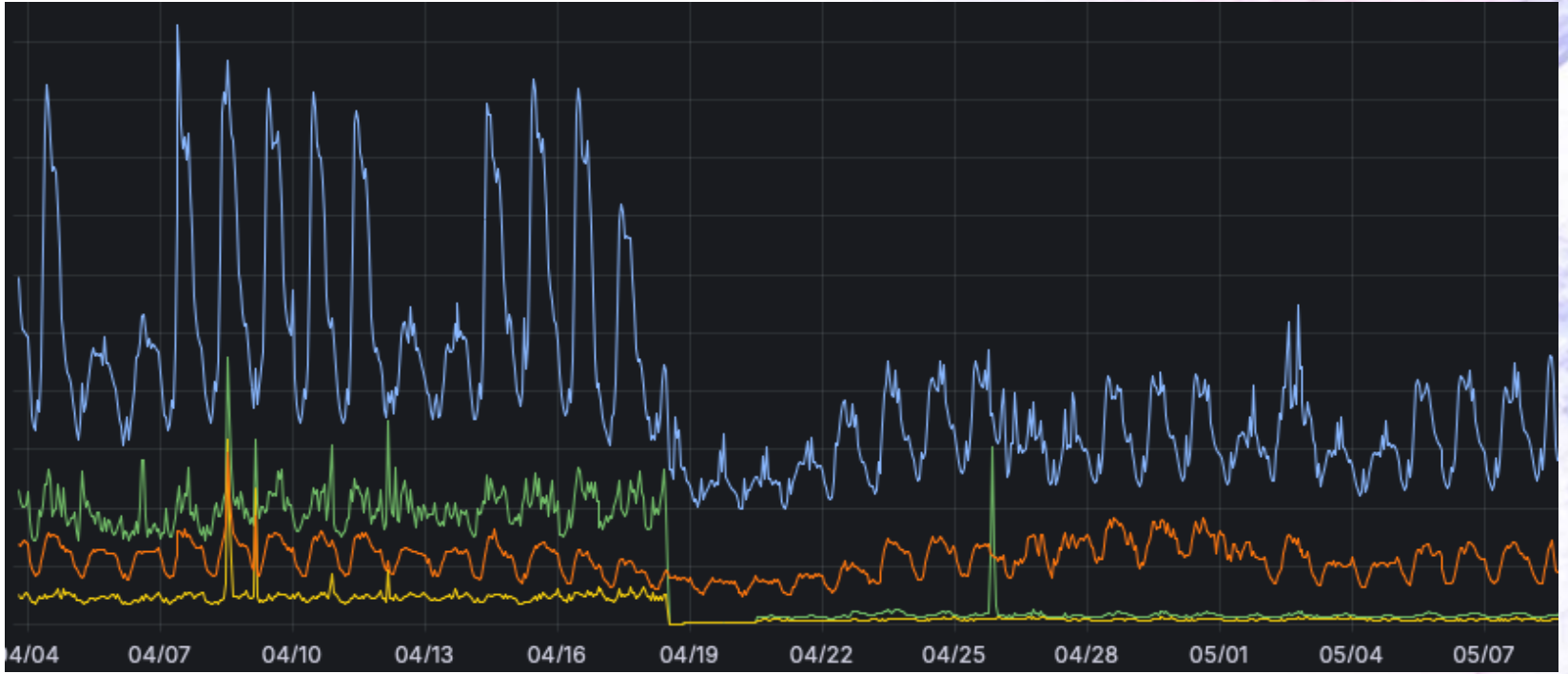
Why go with removing DS records?

- After evaluating different methods for doing this change, TRAFICOM chose the option with smallest total risk
  - Remove DS records from the root for algorithm switchover
  - Runner-up was waiting until next signer hardware refresh
- Primary reason:
  Our test system is not identical with production
- Secondary reason:
  OpenDNSSEC's documentation is scarce and partially outdated

Outcome of the rollover

- .fi was without DNSSEC for about 7 days over Easter
  - Mainly caused by 2*2 * TTL + IANA root zone update delay
- TRAFICOM has heard of no operational issues caused by this change
  - No outages have been reported to TRAFICOM or observed by monitoring
- Some anycast server nodes of e.fi were briefly serving old (incorrect) NSEC3 data
  - SOA serial and RRSIGs were updated, but some NSEC3-records were still from alg 8 zone
  - This was fixed after e.fi operator forced a zone flush on all their nodes

Difference in DNS queries for single node



Blue: V4/UDP Orange: V6/UDP Green: V4/TCP Yellow: V6/TCP