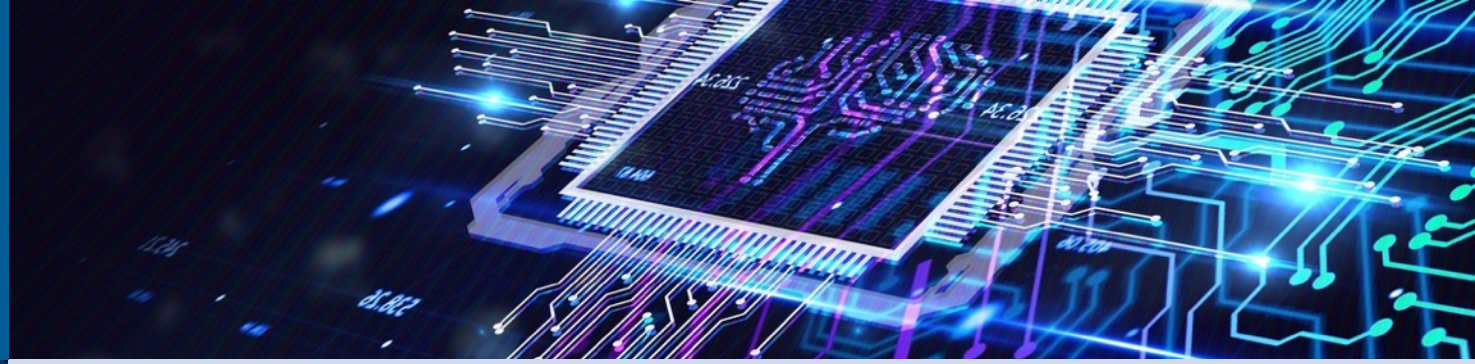
CSC

ICT Solutions for Brilliant Minds



Algorithm rollover at .FI

ICANN83 Policy Forum, 9.6.2025
Juha Suhonen / CSC

CSC – IT Center for Science

CSC is a company entrusted with special state assignments, owned by the state of Finland and Finnish higher education institutions.

- → CSC operates Finland's R&E network Funet
- → CSC hosts Finland's supercomputers & European LUMI

- → CSC has one of the world's most eco-efficient data center environments
- → CSC is a non-profit state enterprise

→ Our primary customers are the Ministry of Education and culture and organizations in the field, higher education institutions, research institutes and public administration

- → CSC connected Finland to Internet in 1988
- → Linux kernel was originally released on nic.funet.fi

Responsibilities regarding .fi

- TRAFICOM (Finnish Transport and Communication Agency)
  - Owns .fi in IANA
  - Owns and operates .fi domain registry (registry portal, EPP, WHOIS, RDAP, …)
  - Has legal obligations as specified by Finnish law 917/2014 chapter 21 (".fi domains")

- CSC (CSC – IT Center for Science Ltd)
  - Operates .fi primary dns ("a.fi") and DNSSEC signing infra for TRAFICOM

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:
  We do not have a test system that is identical with production
- Secondary reason:
  OpenDNSSEC's documentation is scarce and partially outdated

Importing HSM keys to OpenDNSSEC is difficult

- Keys in HSM modules were generated in a key ceremony during initial setup, after this HSM module key management was permanently disabled
  - ECDSA keys had been pre-generated to the HSM modules ..
  - .. but we couldn't test importing these keys to OpenDNSSEC
- OpenDNSSEC has "ods-enforcer key import"
  - All imported keys were also immediately taken into use
- In the end, keys were manually inserted into `hsmKeys` table
- Backup plan was to clear HSM modules and hold new key ceremony, letting OpenDNSSEC generate & store new keys during the ceremony

Timeline of the implementation

Week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
16	DS removal request sent to IANA		DS records removed from root	(2x ttl)	Unsigned zone published	(2x ttl)	ECDSA –signed zone published
17	New DS records submitted to IANA		DS records added to root				

Monitoring before and during change

- RIPE Atlas network was used to monitor .fi zone before and during change
- Each publicly visible step was preceded by a 5000 probe measurement

- Are almost all probes seeing correct (not too old) .fi SOA serials?
  - Some probes are behind DNS servers that cache for too long
- Are any probes seeing historical DS records for .fi in root zone?
  - About 10 % of probes always get SERVFAIL / other error when asking for DS records

Noted issues

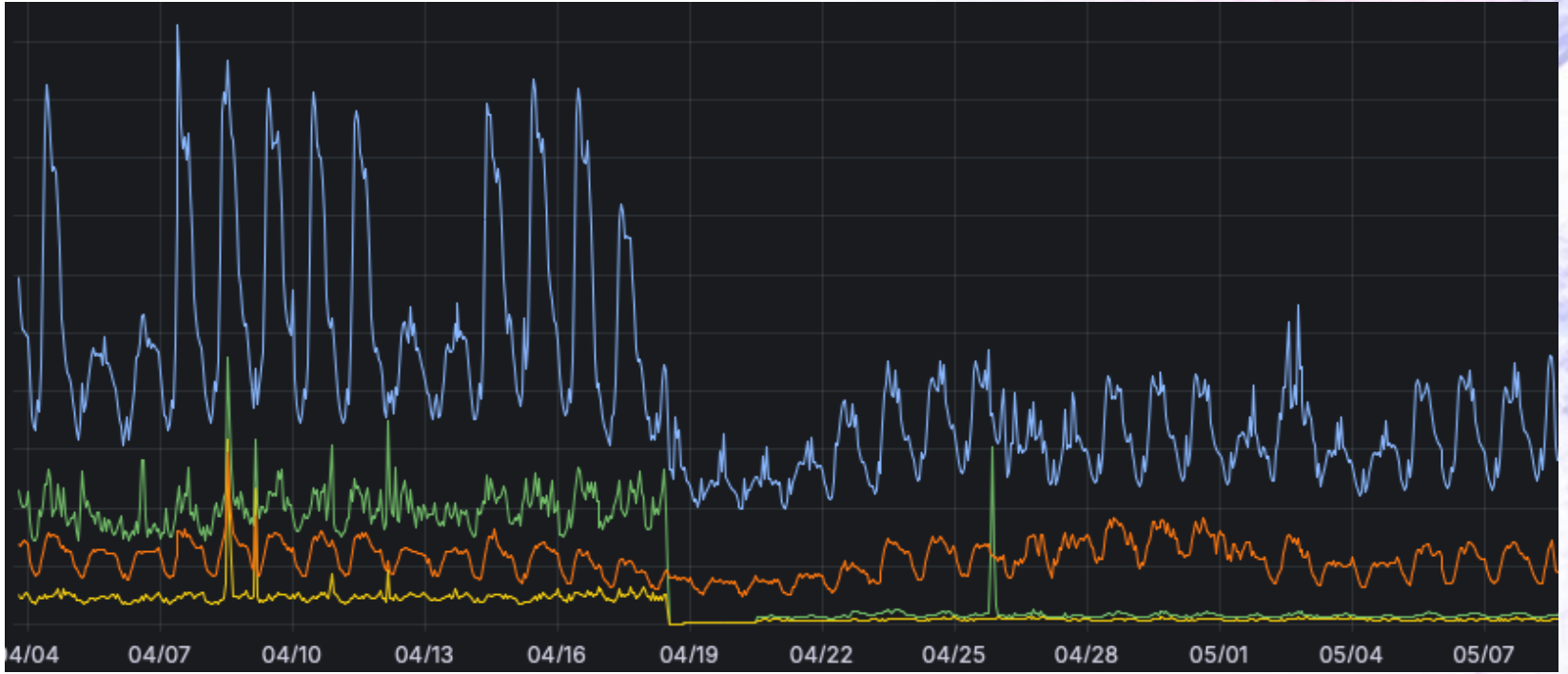
- TRAFICOM has heard of no operational issues caused by this change
  - No outages / other problems have been reported to TRAFICOM or observed by monitoring

- 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
  - TRAFICOM has gotten no official explanation from them
  - Our assumption is that their internal process converts incoming AXFR to IXFR and failed when too many changes were introduced at once

What would be needed for our next algorithm rollover?

- Test system that 1 == 1 matches production
  - Needs to be considered during HW procurements
- Up-to-date and complete documentation for signing software
  - Preferrably also the internals, for example database structure and state machine
  - Including examples of "how to do algorithm roll-over safely"
- Requirement to have RRSIGs with **all** published DNSKEY algorithms causes additional complexity that we'd prefer to avoid if we need to rollover algs again
  - Ideally next rollover would be timed to happen during HW refresh – old/new systems will use different algorithms and only cross-sign each others' keys

Difference in DNS queries for single node



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

CSC

ICT Solutions for Brilliant Minds

Questions? Comments?

Thank you for listening