Postfix's multi-signer transition

DNSSEC and Security Workshop @ ICANN 85

Carsten Strotmann, Patrick Koetter, sys4 AG

CREATED: 2026-03-09 MON 18:51

About

- Experiences when moving DNSSEC signed domains between signers
- Domains for the "postfix" open source mail server https://postfix.org
    - Postfix was the first MTA to support DANE: people are watching, kind of a "role model"
    - "if ***they*** screw up DNSSEC, nobody can operate DNSSEC"

Team

- *Patrick Koetter* (co-author of the Postfix book, head of sys4 AG, active in the smtp mail ecosystem, proponent of DNSSEC and DANE)
- *Wietse Venema* (primary author of the postfix MTA software, http://www.porcupine.org/wietse/, owner of the postfix domains)
- *Peter Thomassen* (co-operator of deSEC.io, a non-profit DNS and DNSSEC hosting service)
- *Carsten Strotmann* (supporting DNS admin for `postfix.*` domains)

History

- The postfix domains were hosted on two DNS server by Wietse Venema since around 1998
- DDoS attacks against the `postfix.org` domain in 2022
    - website, mailinglist and mail-server not reachable for some amount of time
    - we never learned why `postfix.org` was attacked

- sys4 AG helped with DNS expertise and more DNS server, DNSSEC signing.
    - DDoS continued in 2023, but did not bring down the domain anymore

Learnings during the DDoS

- The DDoS was mostly IPv4
- Most Internet DNS-Resolver in the Internet are Dual-Stack
    - Certainly the large ones

- Running part of the authoritative DNS server IPv6-only made them unreachable for these DDoS attacks
    - Domains still visible for users
    - Of course, DDoS attacks might change, but it worked in 2022/2023
    - DDoS attacks stopped in Summer 2023 and never came back

Infrastructure 2022-2025

- Six DNS server (2x Europe, 2x Americas, 2x Asia)
    - traditional networking, no anycast
- Hidden-Primary DNSSEC signer
    - `postfix.*` domains were DNSSEC signed in 2023
- *Ubuntu LTS* with *BIND 9* and *OpenBSD* with *NSD*

Moving to deSEC.io

- Because of NIS2 regulation, sys4 can't afford to offer DNS hosting anymore
    - DNS hosting has been always "pro bono" for open source projects
- deSEC is offering a free and technically better DNS hosting (anycast)

Challenges

- *deSEC.io* has it's own DNSSEC signing infrastructure
  - can't (easily) import existing private keys
- The `postfix.*` domains are highy visible by a community of MTA and DNS admins
  - We didn't want to remove DNSSEC during the transition to *deSEC.io*
  - Why? We wanted to show it is possible to uphold DNSSEC security even during migration

How we did it (1/2)

- Imported the zone data (minus keys and signatures) into the *deSEC.io* system
- Imported the current KSK DNSKEY RR into the new zone at *deSEC.io*
- Imported the new CSK DNSKEY from *deSEC.io* into the old zone on the hidden primary
- Wait for the DNSKEY set to update in the resolver caches

How we did it (2/2)

- Add the DS-Record for the new CSK (*deSEC.io*) into the parent
    - Wait for the DS-RRSet (old and new DS) to be in the resolver caches

- Switch the NS-RRset for delegation in the parent zone to *deSEC.io*
- Wait and observe
- Remove the old DS-records from the parent, remove the old infrastructure

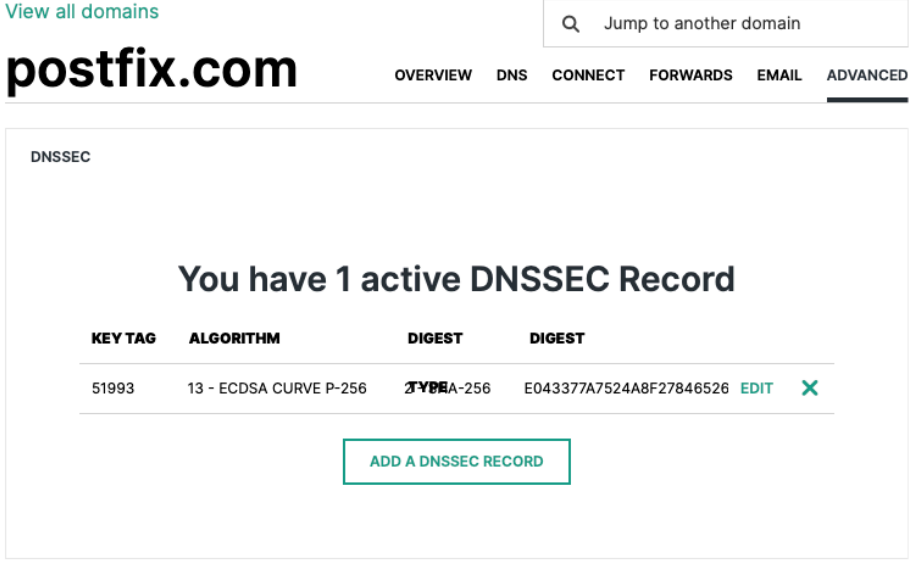
Testing

- `postfix.org` is the main production domain
- we used `postfix.com|net|co.uk|org.uk` for testing

Issues (1/6)

- We migrated `postfix.org`, `postfix.net`, `postfix.com`, `postfix.co.uk`, `postfix.org.uk`
- None of the parents (TLDs) offer DNSSEC DS-record automation (RFC 8078) https://github.com/oskar456/cds-updates
- Different registrars, different Web-UIs for managing DNSSEC

Issues (2/6)


View all domains
Jump to another domain
postfix.com
OVERVIEW
DNS
CONNECT
FORWARDS
EMAIL
ADVANCED
DNSSEC
You have 1 active DNSSEC Record
KEY TAG
ALGORITHM
DIGEST
DIGEST
51993
13 - ECDSA CURVE P-256
2 - SHA-256
E043377A7524A8F27846526
EDIT
ADD A DNSSEC RECORD

Issues (3/6) - "add" means "replace"

- The "add" button actually "replaces" the previous DS-record
    - Replace was done immediatly, breaking DNSSEC :(
- Registrars "invent" new DNSSEC terminology, very confusing
    - Delegation-Signer is called "DNSSEC Record"
- In the end, the new DS-record was manually added by the registrars support

Issues (4/6) - Web-UI not showing the real data

- In one registrars Web-UI, managing DS- and NS-Record-Sets was a challenge
    - You add all DS- and NS-records, the Web-UI looks good
    - You hit "submit"
    - You observe that the state in the DNS changes, but not to the state seen in the Web-UI
        - the inconsistency between webs UI state and DNS state was disconcerting

Issues (5/6) - Web-UI not showing the real data

- DNSSEC is considered to be complicated and error-prone.
    - This narrative keeps people from adopting DNSSEC and keeps them from changing settings in production.

- The User Interface (here: Web-UI) contributes to the narrative because actions don't do what they say and the state after a change is unclear.
- The User Interfaces should produce certainty in actions and states.

Issues (6/6) - Web-UI not showing the real data

- In one registrars Web-UI, managing DS- and NS-Record-Sets was a challenge
    - You reload the Web-UI, and it shows the state as seen in the DNS (not what you entered)
    - Different result every time, not deterministic
    - Solution: remove all records, submit, enter all records, submit again
    - DNSSEC breaks for some amount of time :(

Conclusion

- Moving DNSSEC signed zones is a challenge, because of bad management software at registrars
- DS-Record automation (RFC 8078) would help, but not many TLDs support it
- Registrars still treat DNSSEC as an "excotic add-on than nobody really wants"
    - DNSSEC support at registrar level is almost non-existent