p-square
IT Consulting & Managed Services

DNSSEC at Scale

Enabling Signing Across 5,500 Domains in the Real World

Jens Hoffrichter | p-square GmbH

June 8, 2026

About me

Jens Hoffrichter

Managing Director, p-square GmbH

- Specialized consulting and operations for managed DNS, SMTP, and DDI infrastructure
- Working in enterprise environments: automotive, banking, manufacturing
- Have been Hostmaster and Postmaster for a German DAX automotive company

Storytime!

A major automotive company with a large internet DNS portfolio:

- **5,500 DNS zones** across a highly diverse set of TLDs
- Authoritative DNS already migrated to a cloud DNS provider
- Management via YAML zone files, Terraform, and GitLab CI/CD
- DNSSEC: On one of them

The mission: enable DNSSEC signing across the entire portfolio.

Getting the green light

Even with a clear security benefit, enabling DNSSEC required **significant internal convincing** at the customer.

- DNSSEC was not seen as urgent — "it's been fine without it"
- The green light ultimately came via **BSI compliance requirements** and mail domain security
- Rollout to the full portfolio was approved only as "do what doesn't cost money first"

DNSSEC may be a no-brainer for DNS operators. It is not a no-brainer for enterprise decision-makers.

How hard can it be?

The theory is simple:

1. Enable DNSSEC signing on the zone at the cloud DNS provider
2. Retrieve the DS record
3. Submit the DS record to your registrar
4. Verify the chain of trust
5. Done.

Now repeat 5,500 times.

First surprise: The registrar API gap

First surprise: We could not submit DS records via API for many TLDs at our largest registrar.

- Whether API-based DS submission works depends on each **country's registry**
- Many registries — especially smaller ccTLDs — do not support it
- Our registrar's policy for manual submissions: **"We don't do that."**

For roughly 200 domains, we had no automated path to DNSSEC enablement with our existing registrar.

We needed to transfer those to a secondary registrar who either supported automation for that registry, or did manual submission.

The chain of intermediaries

For some ccTLDs, even a willing domain service provider doesn't have direct registry access.

Example: .cn domains (China)

Customer → p-square → Service Provider (Germany) → Registrar (Brandma, China) → Registry

- DS records communicated via **email** through the chain
- Each hop is an opportunity for copy & paste errors or misunderstandings
- And errors **did** happen

Time zones will bite you

When a DNSSEC configuration breaks on a domain managed through intermediaries in a distant time zone:

- **Brazil example:** Misconfiguration wasn't detected until their next business day
- Rollback required the same chain of intermediaries
- Extended downtime before resolution

Lesson 1: Plan DNSSEC enablement timing around the business hours of every party in the chain, especially for production and mail domains.

Lesson 2: For business critical domains, make sure to do it live, together - so you can immediately verify

TTLs you don't control

When something goes wrong, rollback speed depends on the **DS record TTL at the parent zone**.

- This TTL is set by the **TLD operator**, not you
- Your own zone TTLs (e.g. 600s or 3600s) are irrelevant for DS propagation
- Some TLDs set DS TTLs to **86,400 seconds** (24 hours)

A mistake made on a Friday afternoon in a distant time zone can mean **days of impact** before caches clear and rollback takes effect.

DS record vs DNSKEY confusion

One registrar just needed the **DNSKEY** - that was all they needed for signing.

So we began sending out the DNSKEY to other registrars.

But the registries need the **DS record** — a hash of the zone name + the key.

- The DNSKEY might be the same for every zone
- The DS record is **different for every zone**

When we were sending out the DNSKEY to the registrar, and the registry only accepts the DS record - they need to do the hashing themselves. Which can lead to more errors.

Lesson: Don't assume that what works at one registrar is the same at others - verify!

The .cloud outage

The registrar portal for .cloud had an **ambiguous field label** — it said something like "DNSSEC Key" rather than "DS Record."

The registrar entered the DNSKEY instead of the DS record.

Result: Chain of trust broken. Production domain unreachable.

A registrar domain specialist later questioned why the DS record differed between two domains — not knowing the hash includes the zone name.

These are the people we depend on to get DNSSEC right.

Registries that wake up

DNSSEC enablement counts as a **domain update** at most registries.

For domains registered years ago, this can trigger:

- Requests for **updated admin contact ID documents**
- Demands for current **trade registry numbers**
- Other compliance requirements that changed since original registration

Nobody asked for any of this while the domain sat untouched. The moment you modify anything: **"While we have you..."**

This blocks the rollout in ways no DNS expertise can predict.

The cost surprise

Not every TLD treats domain updates as free.

- Major TLDs (.de, .com): no charge
- Many smaller/exotic TLDs: **€30–50+ per update**
- Multiply by dozens or hundreds of domains

What started as a security project now needs **internal budget approval** at the customer — a political conversation, not a technical one.

Additionally, DNSSEC introduces new resource records into your zones. If your DNS provider charges per RR, you might hit limits or incur additional costs.

Our approach: Enable DNSSEC first on all domains where it costs nothing. Negotiate budget for the rest separately.

TLDs where DNSSEC is impossible

Some domains simply cannot be signed today:

Registry doesn't support DNSSEC:

- .ae (UAE) — the registry does not offer DNSSEC at all

Algorithm mismatch:

- .co.kr — registry requires algorithm 8 (RSA/SHA-256)
- Our cloud provider signs exclusively with algorithm 13 (ECDSA P-256)
- Incompatible. No workaround without changing DNS provider.

These domains must wait for the registry to modernize or the DNS provider to change.

Operational strategy

This was the strategy we finally settled on.

1. **Start with mail domains** — highest security value, strongest compliance argument
2. **Group by registrar and TLD** — batch requests to minimize intermediary overhead
3. **Prioritize API-capable TLDs** — get volume done fast, handle manual cases separately
4. **Schedule around time zones** — enable during overlapping business hours with all parties
5. **Budget exotic TLDs separately** — don't let cost discussions block the free domains

Key takeaways

- DNSSEC at scale is a **registrar logistics project**, not just or even mainly a DNS project
- The **domain industry supply chain** is deeper and messier than you expect
- Human error in the chain is inevitable — plan for rollback at every step
- **Know your constraints** before you start: provider billing, registry support, algorithm compatibility
- Automate verification — you cannot manually check 5,500 domains
- Get organizational buy-in early — the hardest part may not be technical

Wishlist

For Registries

- Make automation as easy and frictionless as possible
- Support CDS/CDNSKEY
- Pricing for updates

For Registrars

- Automate everything!

Contact

Jens Hoffrichter
p-square GmbH

jens.hoffrichter@p-square.de

https://p-square.de (DE)
https://p-square.digital (EN)

https://www.linkedin.com/in/jens-hoffrichter/