The .SE DNSSEC Signing Incident

February 2022

Johan Stenstam

The Swedish Internet Foundation

June 7, 2022

Friday Afternoon, February 7, 2022 We Had a Problem

In the afternoon IT Operations became aware that a version of the `.SE` zone with several thousand broken DNSSEC signatures was published on the public Internet.

- Trying, repeatedly, to generate a new signed zone failed. New signatures generated by the HSMs were invalid.
- "Rolling back" (to a known good version of the zone) was not an option, because of multiple external providers of global anycast.
  - I.e. the `SOA` serial logic would make such an operation both time consuming and complex.

So, in practice, the only way forward was, well, "forward".

- New, correct, signatures, **must** be generated.

What Had Happened?

The Swedish Internet Foundation runs multiple physical HSMs in a high-availability cluster configuration.

- Each zone (in our case `.SE` and `.NU`) has a dedicated partition in the HSMs (i.e. the keys for each zone are completely separate from each other).
- The HSMs communicate with each other to synchronize keys, etc.
- Regenerating signatures for `.SE` resulted in new, broken signatures.
- Regenerating signatures for `.NU` resulted in new correct signatures.

Worst of all: both HSMs exhibited the exact same behaviour. I.e. it was not a case of hardware failure in a single HSM.

Some Context

`.SE` was the first ccTLD to be signed and that was a long time ago.

At that time the tools were not nearly as mature as today.

- This lead to a completely homegrown zone generation and signing pipeline.
- While parts have been upgraded over the years, the underlying infrastructure and pipeline design was very old.

We had clearly fallen into the trap of "don't touch it, it works".

What About Validating Signatures Before Publication?

Yes.

That would have saved us.

But, unfortunately, the series of tests that were made before publication of a new zone did not include signature validation.

- As far as I understand, the original reason was that signature validation for the entire `.SE` zone simply took too long. Then.
- With today's hardware this is no longer true, but the test was never added to the pipeline.
- See the part about "don't touch it, it works".

Also, the scenario that the old pipeline was designed to deal with included one HSM failing **with an error** (and the other taking over), not both of them failing silently at the exact same time.

How Did The Incident Get Resolved?

The zone signing pipeline for **.SE** is designed around OpenDNSSEC as the signer software, with two Thales Luna HSMs for key generation, storage and signing operations.

- Various tests, including restarting OpenDNSSEC, breaking apart the HSM cluster into separate HSMs, etc, **did not resolve** the problem.

Then the more aggressive action of physically restarting the first HSM was tried.

- That HSM started to work correctly after the reboot.
- Then the second HSM was restarted (and that also came back to correct operation).

Impact of the Incident

The problem had a duration of about 13 hours, from the time of the first invalid signature being published around 9am (new zone publication was halted from 2pm) until a zone with all signatures valid was published around 10pm.

- As a matter of principle, all delegations are of course equal and important.
- But, even so, some delegations do have a greater impact on "society".
- At most 9092 invalid signatures were published.
- None of the invalid signatures involved a delegation of "national importance".

This was "pure luck" on our part (if we should call it that). Or, "bad luck" on the part of the affected delegations.

Aftermath

It's been about four months and apart from various analyses, reports, etc, the current status is:

- Validation of generated signatures was added to the pipeline the same weekend.
- A completely new zone generation and -signing pipeline has been designed and it will be implemented during autumn 2022.
- No code from the old pipeline will be kept.

Root Cause Analysis

The first thing to check was OpenDNSSEC.

- Thorough analysis of has concluded that OpenDNSSEC is not the root cause of the invalid signatures.

The second thing was the HSMs.

- As both HSMs were rebooted, and have worked correctly since, we have been unable to reproduce the behaviour from February.
- The HSM vendor obviously have a difficult task trying to explain a behaviour that is not reproducible.
- In spite of the absence of such an explanation, this is where we concluded that the root cause lies.

A further concern is the fact that **both** HSMs started to misbehave together in conjunction with the error not being a hardware failure.

- The HSMs communicate privately to synchronize keys.

Conclusions And Lessons Learned

`.SE` was the first ccTLD to be signed and that was a long time ago.

- The zone generation and -signing pipeline has of course been updated and modified since then...
- ...but over time a mind set of "don't touch it, it works" was established. That's dangerous.

Apart from that, there are also lingering concerns about the fact that the collective behaviour of multiple HSMs at the same time has not been satisfactorily explained.

- The good news (in the `.SE` case) is that we can halt zone publication for hours (or even days if needed).
- ...so we compensate by deploying more rigorous pre-publication testing.

Thanks!

Johan Stenstam

DNS Apprentice

johan.stenstam@internetstiftelsen.se