InternetNZ .nz DNSSEC Incident

May 2023

Felipe Barbosa

What we'll cover

- Who is InternetNZ
- .nz registry and DNS overview
- The incident
- The cause
- Next steps
- Lessons learned

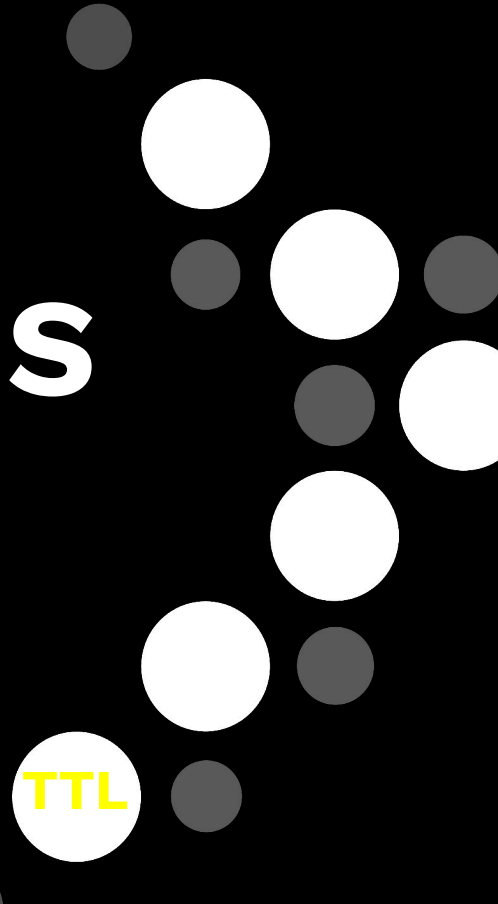
InternetNZ and the team behind .nz

InternetNZ is a non profit and the home and guardian of .nz

We have an operations team of five that handles all aspects of running infrastructure, network, virtualization and applications.

i.e. Registry, DNS and DNSSEC signing

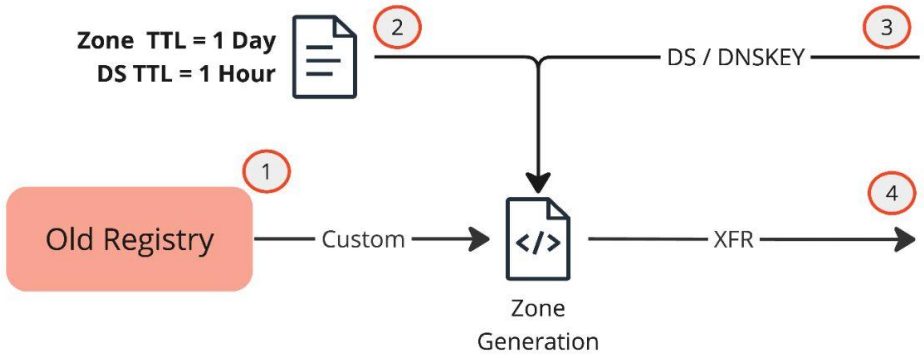
.nz registry and DNS overview

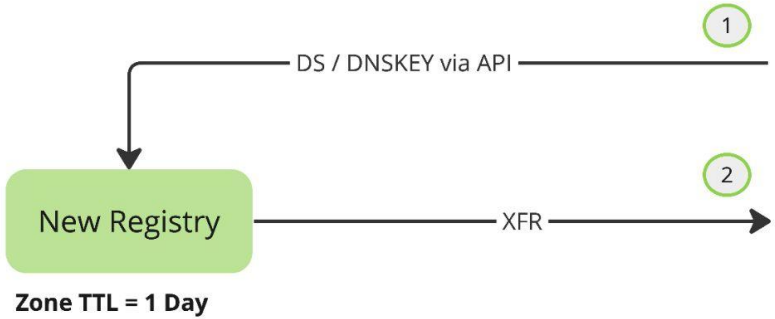


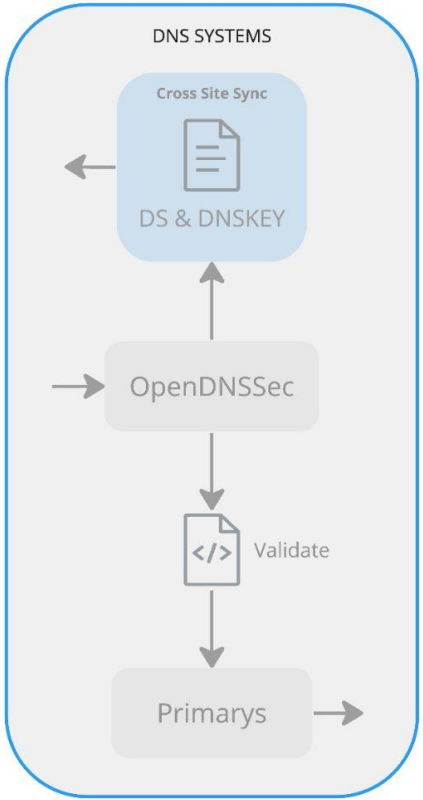
The .nz registry replacement

- Replaced inhouse registry with the new external registry platform in a 3 year project
- Go live was 1 November 2022
- Greenfields build, new racks, new network, new servers, new operating systems and new registry software
- Integrated with existing DNS infrastructure (Multi-signer model 2, RFC8901)
- Zone generation process changed

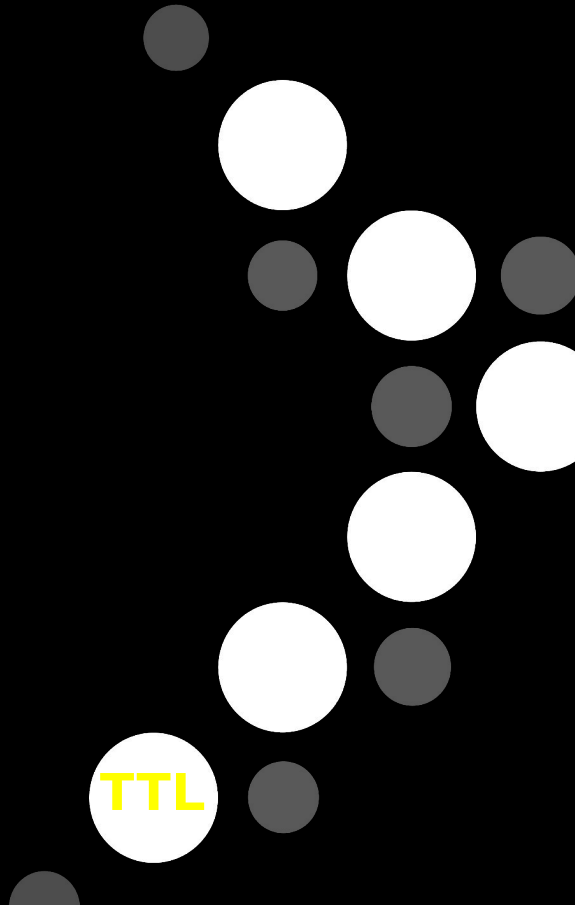
Zone generation process overview







The incident



KSK rollover operation begins

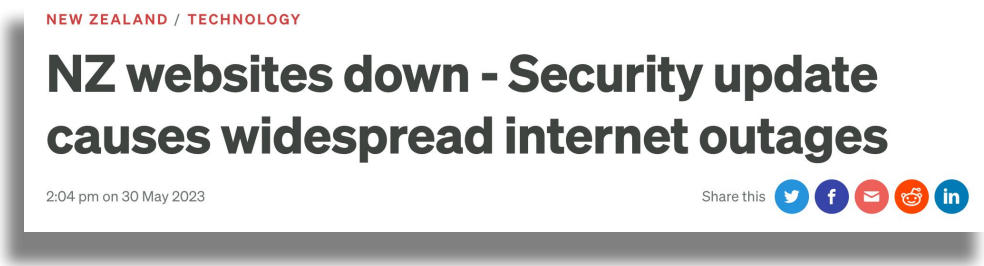
- ac.nz rollover started early
- Problems reported by a 3rd party
- Internal investigation started
- We couldn't reproduce the problem

KSK rollover operation continues

- Remaining 14 second level domains progressed, except for .nz top level domain
- Problems reports escalate
- More investigation
- We couldn't reproduce the problem

Following morning: public response

- Calls from New Zealand media outlets on Tuesday morning. Lots of incorrect speculation from the media
- Most of the morning spent drafting the press release message
- Articles in major New Zealand news outlets



NEW ZEALAND / TECHNOLOGY

NZ websites down - Security update causes widespread internet outages

2:04 pm on 30 May 2023

Share this

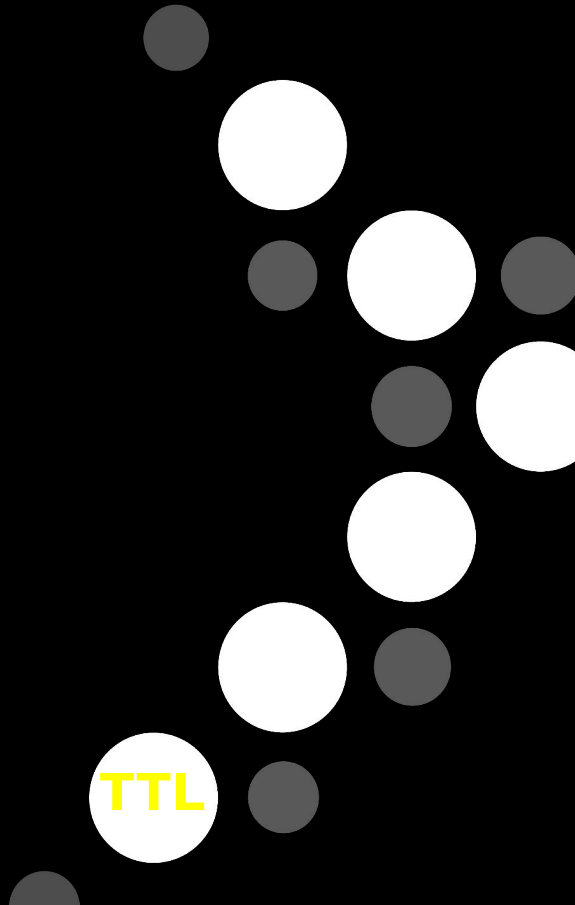
Widespread website, app outages: InternetNZ apologises for 'change of house keys' gone haywire

Capturing the symptom

- Identified the reported problem internally
- Reproduced the problem internally
- Observed **ServFail** answers from **recursive server**
- Logs revealed

```
validating net.nz/DNSKEY: no valid signature found (DS)
no valid RRSIG resolving 'net.nz/DNSKEY/IN'
```

The cause



The cause: 1 day != 1 hour

- Old registry set the TTL for DS records to one hour, in the new registry DS records inherited the zone default TTL of one day
- Resulted in misalignment between OpenDNSSEC policies and zone DS record TTL
- Led to the early removal of the old DNSSEC KSK, causing problems for resolvers with cached records

Available options

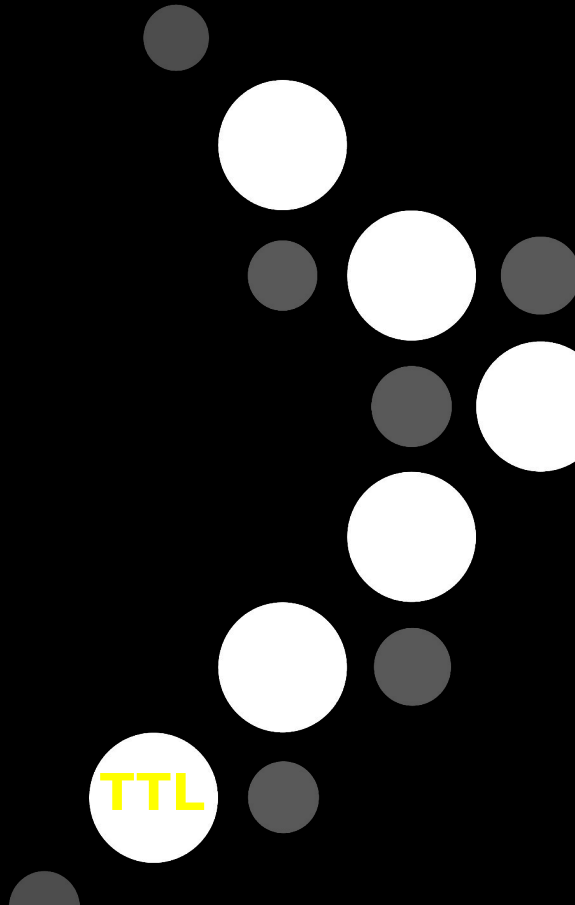
- Site switching
- Recover the keys that had reached dead state
- Engage the technical community directly / request to flush caches and having the prebuilt channels to do that
- Go unsigned

We decided to wait, communicate and advise (flush cache) etc..

KSK rollover operation ends

- TLD nz KSK role finished
- Paused zone distribution to the Internet
- Manual verification and analysis of every zone DS and DNSKEY
- Resumed zone distribution to the Internet
- No problems reported

Next steps



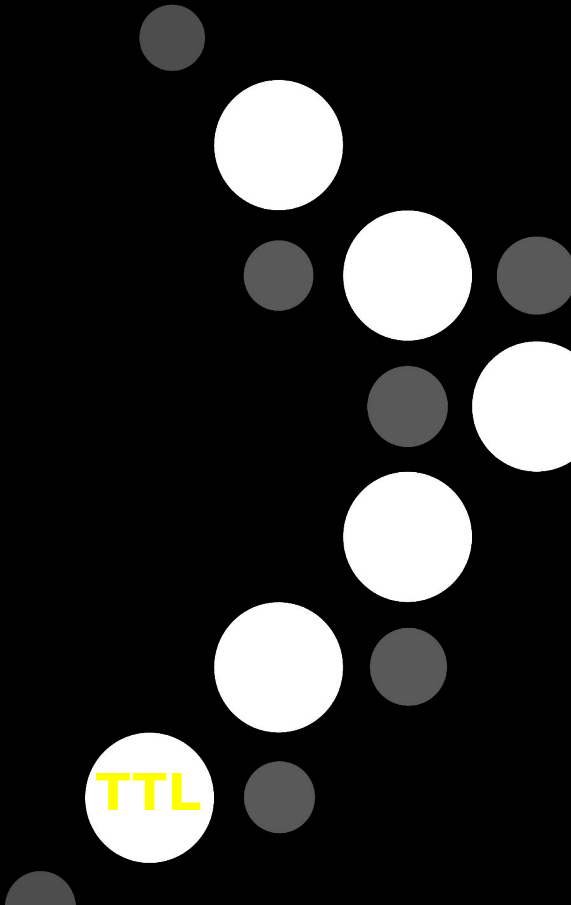
What's next - technical

- Review and change of OpenDNSSEC policy
- In discussion with software vendor for potential customisation in zone generation
- DNS review/HSM refresh project underway to align with new infrastructure
- Indirect monitoring, through recursive servers

What's next - public response

- Prompt communication with the technical community via established channels
- Prepared messaging and plans that can be used in the future, avoiding the general public information void
- Proactive interaction with the local community about routine operations
- InternetNZ Council commissioned an independent report

Lessons learned



Reflections

- Have an incident response plan and practice it
- Issues can still occur despite extensive testing, and established process need regular review
- A united team helps a lot in crisis situations
- Use **short TTLs** for your **DS records**
- The situation can always get worse (baby steps)

Thank you.

Resources

InternetNZ Incident Report

Felipe Barbosa
felipe@internetnz.net.nz

Josh Simpson
josh@internetnz.net.nz

internetnz