Report of External Review into .nz DNSSEC Chain Validation Incident on 29-30 May 2023

Report prepared for InternetNZ Council

August 2023

v1.0

Independent Reviewers:

Ewen McNeill, Naos Ltd (“Technical Reviewer”)

Laura Dempsey, Cubal Team Ltd (“Human Factors Reviewer”)

Table of Contents

Executive Summary

InternetNZ operate the DNS registry for the .nz CCTLD (see 20), which since 2011 has published DNSSEC signed records to the DNS; see 21. Over 85% of Aotearoa | New Zealand Internet users access the Internet through DNS resolvers which rely on consistent DNSSEC records being published by the .nz DNS registry; see 47.

On Monday 2023-05-29 InternetNZ caused internally inconsistent DNSSEC information to be visible to the caching recursive DNS servers used by end users, during an unnotified annual maintenance task; see 30. The inconsistent information was visible for up to 19.5 hours for "ac.nz" (see 46), and up to 14.75 hours for other .nz domains (see 46). This resulted in .nz DNS information being considered "bogus" until the inconsistent information expired or was flushed from DNS server caches by third party DNS server operations (eg at ISPs); see 54.

The Incident occurred because InternetNZ had not updated its maintenance procedures, or the DNSSEC signing configuration, to reflect new "DS" "TTL" record values published into the DNS by their new "IRS" registry software platform deployed in 2022; see 55. There were no technical controls (see 63) or administrative controls (see 77) to ensure consistent configuration or processes. These values were also inconsistent between 2014 and 2018, fortunately without incident; see 55.

Both parts of the incident were avoidable (see 63), but once the incident was in progress, it is understandable the .nz Operations Team were unable to identify *both* technical causes in time to safely recover from the wider .nz KSK Incident before it affected end users; see 57.

InternetNZ communication to ISPs was prompt, but InternetNZ communication to the wider Internet community only began 10 hours into the main incident; see 44. Initial wider communication lacked detail, but it was updated repeatedly on Tuesday 2023-05-30; see 44 and 34.

Key recommendations:

- High impact risk infrequent maintenance should be notified in advance
- High impact risk tasks should be done by multiple people together
- Handle unexpected symptoms during maintenance as "an incident"
- Formalise communication channels to recursive DNS server operators
- Ensure OpenDNSSEC "DS" configuration to matches DNS reality
- Add guard rails around OpenDNSSEC commands
- Document change of "DS" TTLs in .nz zones since November 2022
- Validate production change process with a true "canary" rollover
- Develop a process to ensure BAU task prerequisites are completed before BAU tasks
- Support .nz Operations Team to build and use their international network
- Review and Update the Business Continuity Plan

See Report recommendations for future improvement for additional recommendations.

Introduction

Purpose of this Report

Over the period of 29 and 30 May 2023, an incident ("the Incident") took place during an annual maintenance procedure to rollover the "DNSSEC" (Domain Name System Security Extensions) key signing keys. The old keys prematurely stopped being used, causing many users to experience failures in the DNS ("Domain Name System") resolution of .nz DNS names. It is estimated this Incident caused some end users to experience problems accessing .nz domains for two periods of up to about 6 hours each ("ac.nz" on 2023-05-29; other .nz domains mostly on 2023-05-30).

InternetNZ recognised the serious nature of the Incident and conducted their own internal review which was published on the InternetNZ website on 26 June 2023 (DNSSEC chain validation issue: technical incident report » InternetNZ).

Along with an internal review, the InternetNZ Council requested an external independent review of the Incident to:

- examine the events leading up to the Incident
- consider the response to the Incident; and
- recommended improvements to prevent similar incidents in the future.

The review was to cover the technical factors as well as the non-technical (business process, human factors) that may have contributed to the Incident.

Ewen McNeill, Technical Consultant, Naos Ltd and Laura Dempsey, HR Consultant, Cubal Team Ltd, were engaged to conduct the review.

Incident overview

The .nz DNS registry information published by the InternetNZ DNS servers is critical national infrastructure for Aotearoa | New Zealand.

Information from the .nz DNS servers is used constantly, 24/7, as part of resolving any DNS name ending in .nz to an IP address. Computers need to obtain these IP addresses to contact any service provided over the Internet which identified by a name ending in .nz. It is not possible to resolve a .nz DNS name without involving information from the .nz DNS servers: this central source of DNS resolution information is the purpose of a DNS registry.

DNS names ending in .nz are widely used in Aotearoa | New Zealand, for government and business services, including many with critical importance to the day to day lives of citizens and residents of Aotearoa | New Zealand. Many organisations consume their own DNS names in part through the records published in the .nz DNS registry (both internally and, eg, staff working from home); this "look up DNS names via the public records" is also Internet recommended best practice.

InternetNZ, through former subsidiaries and more recently directly, has operated the .nz DNS registry and related .nz DNS servers, for over 25 years (since the .nz CCTLD was re-delegated to InternetNZ by IANA by the former operator of the .nz DNS registry, the University of Waikato, in 1995).

Until 29-30 May 2023, InternetNZ (via subsidiaries and then directly) had operated the .nz DNS registry, and related DNS servers, successfully, with no incidents resulting in the difficulty or inability to resolve .nz DNS names.

The Incident of 29-30 May 2023 was the first, and only, major incident affecting the ability to resolve .nz DNS names during the time that InternetNZ has operated the .nz DNS registry.

The Incident of 29-30 May 2023 resulted from actions taken by InternetNZ during an annual maintenance procedure (a "DNSSEC KSK rollover"), *following processes and using configuration that had been proven to work successfully in previous years*.

Unfortunately these processes and configuration *had not been updated* to reflect changes made to other .nz DNS registry systems, which had occurred since the last annual "DNSSEC KSK rollover" maintenance procedure (a year earlier). This resulted in some steps being performed by automation (and in one case manually, as a test) earlier than it was safe to perform those steps in the new circumstances.

As a result of this 29-30 May 2023 Incident, information *internally inconsistent with cached records* was visible for the .nz second level domains (ac.nz, .co.nz, .govt.nz, .net.nz, etc) between the late morning of Monday 29 May 2023, and the early afternoon of Tuesday 30 May 2023, to caching recursive DNS servers around the world.

This inconsistent DNS information being visible caused difficulty resolving .nz DNS names through (DNSSEC) *validating* recursive DNS servers. *Validating* recursive DNS servers check that the visible DNS information, that they obtain from DNS servers like the .nz DNS servers, is internally consistent. Those validating recursive DNS servers that saw inconsistent information for .nz DNS names refused to use the DNS answers received from the .nz DNS servers, considering the answers "bogus". This resulted in DNS lookup failures for .nz DNS names via those validating recursive DNS servers for one or more hours (until the cache time on old records expired, or the DNS operator intervened to flush the cache).

Whether or not a particular validating recursive DNS server saw the internally inconsistent information depended on the timing with which it fetched, and cached, the various DNS records involved in the validation process. If it happened to fetch *all* the updated records soon after they were all updated, then it would have seen inconsistent information for little or no time, and the new consistent records almost immediately.

If a validating recursive DNS server happened to fetch some records immediately before they were changed, it may have had an inconsistent view for up to 19.5 hours (ac.nz; 14.75 for other 2LDs), unless some action was taken by the operator of the validating recursive DNS server to force it to fetch all new (and thus consistent) information for the .nz second level domains.

Such manual action to force fetching new information by a DNS server is an unusual exceptional action, only ever required to speed up recovery from a mistake made in DNS server operation somewhere else.

The timing of the visibility of the inconsistent information varied between .nz second level domain, with .ac.nz having inconsistent information visible first on the afternoon of Monday 29 May 2023,

and the other second level domains having inconsistent information visible from late evening of Monday 29 May 2023; the timeline is discussed in much greater detail below.

One of the first actions of the InternetNZ Council committee responding to this 29-30 May 2023 Incident, was to determine that there needed to be an internal review, and an external review, and set in process actions to capture as much information from the Incident as possible. The internal review was completed within a few weeks of the Incident (DNSSEC chain validation issue: technical incident report, published 2023-06-26).

This is the report from the external review, conducted a couple of months after the Incident, in late July 2023 and early August 2023.

All dates and times in this document are given in Aotearoa | New Zealand local time at the time the events occurred. International readers may wish to note that the Aotearoa | New Zealand time zone at all relevant times during the 29-30 May 2023 Incident was UTC+12 (NZST). Times are given in 24 hour format to avoid confusion between morning and evening/night tasks while also translating time zones.

Incident Context Timeline

For background context, we have set out below the past events which were taken into consideration when reviewing the Incident.

2014 **20 February** Time to Live ("TTL") of DS records .nz DNS changed to 1 hour (at request of registrars)

2018: New Zealand Registry Service (NZRS) merged into InternetNZ.

20 June OpenDNSSEC "signer" configuration changed to rely on 1 hour TTL (was 1 day)

2019: InternetNZ started the Mimosa Project to find replacement software for the DNS registry platform.

2021 **December** proposed organisational restructure change document went out for consultation.

2022 **April** Organisational restructure decision announced; senior leadership level now having four puni (teams) Te Puni Whiria | Public Impact, Te Puni Whakawhanake Rawa | Customer and Product, Te Puni Raupā | Organisational Performance and Te Puni Māori.

.nz Operations Team reports to the General Manager of Te Puni Whakawhanake Rawa | Customer and Product

End of April/Start of May new structure came into effect. The leadership team comprises of the Tumu Whakarae | Group Chief Executive and the GMs / heads of each of the puni and the Domain Name Commissioner (who heads the Domain Name Commission) as part of the Group Leadership team. (Please refer to Appendix I for final organisational structure).

The Mimosa Project was largely unaffected in so far as roles involved in the Mimosa Project remained until the new Te Puni Whakawhanake Rawa | Customer and Product General Manager (GM) was appointed to ensure stability during a critical period of delivery for this project.

June Te Puni Whakawhanake Rawa | Customer and Product GM, commenced full time (it is understood they worked part time for a few weeks while transitioning roles). This role leads the .nz Operations Teams, who performed the annual rollover of the DNSSEC keys.

Along with the restructure the following took place:

- Tumu Whakarae | Group Chief Executive (CE)
  June previous CE left the organisation
  June– October interim CE was put in place
  October new CE commenced

- Domain Name Commissioner
  April Commissioner left
  April interim Commissioner was put in place

  September InternetNZ engagement survey took place.

- Internet NZ Registry system
  1 November - New InternetNZ Registry System ("IRS") enters production / goes live.

2023

February InternetNZ meeting with CIRA to move into business as usual report process for the registry. Project wrap up moving into business as usual for the registry. There was a general discussion about the CIRA registration platform using a single TTL value for all record types.

May new Domain Name Commissioner commenced

29 May/30 May The Incident took place.

Time period under review

There were two distinct phases to the technical DNSSEC KSK rollover Incident:

- the ac.nz KSK rollover incident, on Monday 2023-05-29 afternoon (with less widespread impact)
- the other .nz second level domain KSK rollover incidents, with effects noticeable from late evening Monday 2023-05-29 and most widely observed on the morning of Tuesday 2023-05-30

Since the technical and human factors causes of these two phases of the Incident are identical, and the steps leading up to the other (non-ac.nz) .nz second level domain KSK rollover incidents were already well under way when the ac.nz KSK rollover incident was first reported, this review treats

both of these incidents as a single Incident, which spread out over (Aotearoa | New Zealand) two calendar days.

In response to particularly the other .nz second level domain KSK rollover incidents, the InternetNZ internal BCP ("Business Continuity Process") incident response plan was invoked, on the morning of Tuesday 2023-05-30, and soon after the InternetNZ Council BCP incident response plan was also invoked. This led to, among other things, to the OpenDNSSEC "ods-enforcer" process being disabled (from automated runs, then later also disabled for manual runs) to avoid any unexpected key transition steps during the initial Incident review period.

Once the root causes had been identified, with the help of third parties confirming the InternetNZ diagnosis, the InternetNZ .nz Registry returned to "normal operations" two days later on Thursday 2023-06-01 evening after carefully completing the remaining steps of the KSK rollover process by hand (see DNSSEC chain validation issue for .nz status update, and the timeline below for more detail). Some .nz Registry functions relating to DNSSEC "key rollover" have been left paused since the Incident (including the "standby" DNSSEC signer, and ZSK rollovers) pending the outcome of this external review and completing planned changes first.

For this report, the technical incident, and the incident response over the surrounding few days, is all treated as part of "the Incident" under review in this report. The report also examines, in summary, the earlier events leading up to the need for configuration changes to the DNSSEC KSK rollover procedure if it were to be carried out safely on 29 May 2023.

All the new KSK keys for the active DNSSEC signer to use were generated on Friday 2023-05-26, including the new KSK key for .nz and a new KSK key for each of the .nz second level domains, and added to the active OpenDNSSEC "signer" key database as available to be used in future.

As noted in the "Summary of .nz DNSSEC Chain Validation Incident" section at the beginning of the document, the KSK rollover of the .nz top level domain proceeded normally without any incident. We are aware of DNS resolution issues with names in the .nz top level domain during the Incident period, which we believe are due to dependencies on resources (eg, nameservers) under one of the affected second level domains. As a result the KSK rollover of the .nz TLD zone is discussed in the timeline and user impact below, but not specifically described as a part of the Incident itself.

External review process

This review was conducted through a combination of:

- video conference interviews with 7 InternetNZ staff, 5 stakeholders and the Canadian Internet Registry Authority (CIRA) and two members of the InternetNZ Council;
- follow up questions via email, and social media platforms
- detailed review of the console logs, change history, timelines and other technical information surrounding the Incident provided by the InternetNZ
- detailed review of contemporaneous incident discussion in online media, including the NZNOG "Slack" and Geekzone forum, and reporting in professional media
- review of InternetNZ September 2022 Engagement Survey

- review of final decision document *"Decisions: Setting ourselves up for the future"*
- review of the Business Continuity Plan and various operational policies and position descriptions; and
- validating the information provided by InternetNZ against third party sources, eg DNSViz, as much as possible (especially to confirm the timelines and validate the root causes identified)

We would like to commend the InternetNZ Council for realising early in the Incident response process that a serious incident had occurred, that it would need both an internal post-incident review and an external post-incident review, and for immediately capturing as much context as possible at the time. We have seen console sessions and log information that helped establish key details which would have been unavailable but for those prompt actions to enable the review.

InternetNZ, and especially the .nz Operations Team of InternetNZ, have been extremely responsive in providing all information requested, and answering all questions asked. Which has enabled us to build out a more complete picture of both what was *possible* at the time of the Incident, and what *they knew* was possible at the time of the Incident which shaped their immediate response to the Incident.

Technical summary of .nz DNSSEC Chain Validation Incident

On Monday 2023-05-29 InternetNZ started key steps in the annual rollover of the DNSSEC ("Domain Name System Security extensions") KSK ("Key Signing Key") for the second level domains (2LD) of .nz (eg, ac.nz, co.nz, net.nz, org.nz, etc), *following the same process that they had used successfully the previous 5 years*.

This 2023-05-29 DNSSEC KSK rollover *for the second level domains* did not go as smoothly as previous years, resulting in a period where some (but not all) DNSSEC validating resolvers considered the answers returned by the .nz DNS servers to be invalid, and refused to use the answers (declaring the answers "bogus").

Most of the user impact occurred after the second phase of the KSK rollover happened, *automatically*, late on the evening of Monday 2023-05-29, for the bulk of the .nz 2LDs. With the majority of impacted users noticing issues on the (New Zealand) morning of Tuesday 2023-05-30 as they started their day, and possibly in some cases continuing into the very early afternoon of Tuesday 2023-05-30. Technical impacts should have been over by 2023-05-30 13:30, based on DNS record cache expiry times. Most users should have seen the problems resolved by late morning, either due to DNS record cache expiry times or due to prompt recursive DNS operator mitigation steps.

The DNSSEC KSK rollover for the main .nz TLD ("Top Level Domain") proceeded normally and there were *no known issues with that main .nz TLD KSK rollover* itself. Due to the history of the .nz top level domain, which did not allow direct end user registration into the top level .nz zone until recently, DNS resolution of names directly under the .nz top level domain was in some cases also have been impacted by issues with the DNSSEC signing chain of the .nz second level domains, where it relied on systems referenced via names in a .nz second level domain (eg, DNS nameservers).

The exact timeline observed by any user is complicated by the DNS answer caching features, and the timeline is discussed in much more detail below.

The most directly relevant technical causes of the .nz *second level domain* DNSSEC chain validation incident are:

- the old "KSK" ("Key Signing Key") stopped being used for signing the "ZSK" ("Zone Signing Key") *in the second level domains* before *all* validating DNS resolvers were aware that the change to the new KSK was occurring
- the TTL ("Time To Live") value on the DS records in the .nz top level domain, pointing at the .nz second level domains "KSK" values, had changed from 1 hour (3600 seconds) to 1 day (86400 seconds) in November 2022 (but the TTL on the DNSKEY records remained at 1 hour / 3600 seconds)
- since the last annual KSK rollover (mid 2022), on 2022-11-01, InternetNZ deployed into production a new DNS registry system (the "InternetNZ Registry System", IRS) completely replacing the old registry system, the SRS ("Shared Registry System") and a separate DNS "zone build" tool

- because the DNS “zone build” feature was now internal to the new (third party) registry system, InternetNZ had to create a tool to add the “DS” records pointing at the “KSK” values for the .nz second level domains, into the .nz top level domain zone information in the registry, using built in registry API (“Application Programing Interface”) features
- the new registry system DNS “zone build” feature gave all records added to it, *including the “DS” record being added by InternetNZ automation*, a standard TTL (“Time to Live”) value of 1 day (86400 seconds); the previous (“SRS”) registry DNS public gave “DS” records a 1 hour (3600 second) TTL, since 2014
- the InternetNZ managed DNSSEC signing software *configuration* had not been updated to reflect this change (back) to a 1 day TTL (86400 seconds) for the DS records, and the DNSSEC signing software continued to assume 1 hour (3600 seconds, since 2018) when calculating safe times for next steps (eg, stopping signing ZSK records with the old KSK)
- As a result of the DNSSEC signing software stopping using the old KSK for signing the ZSK too soon, based on its outdated configuration values, validating DNS resolvers with a cached copy of the *old* DS record saw a broken DNSSEC trust chain as soon as they fetched a new copy of the “DNSKEY” record for the zone which did not include a signature using the old (cached) expected KSK value.
- The DNSSEC validating recursive servers had problems until the old “DS” records without the new KSK value either expired out of the cache, or were manually flushed from the recursive DNS server cache by third party DNS server operations mitigating the impacts of the Incident.

Systems known to have functioned as designed/configured during the Incident period

For certainty, we record that these systems functioned exactly as they were designed and configured during the Incident:

- The new (2022-11-01 production) InternetNZ Registry System (IRS), based on software provided by the Canadian Internet Registry Authority (CIRA) functioned without any issue, including processing all requests to update DNS information in the registry and publishing DNS zone updates
- The InternetNZ DNS server infrastructure function as normal, without any issue; there was no problems or delays in publishing any updates (except when updates were briefly paused for a maintenance step related to resolving this incident, on the afternoon of 2023-06-01)
- The OpenDNSSEC signing infrastructure functioned *exactly as configured* throughout the Incident, without any problems running commands, or performing the DNSSEC signing (as described above the Incident was caused because *a key configuration value was out of date*)
- The Internet connections for InternetNZ, the IRS registry software, and the various .nz registry DNS servers all functioned without problems
- All commands issued by the Internet .nz Operations Team were issued correctly, following the InternetNZ procedures for a DNSSEC KSK rollover, and following the timings in the existing InternetNZ standard operating procedure for DNSSEC KSK rollovers

The sole *direct* technical cause of the Incident was that the OpenDNSSEC *configuration,* and the InternetNZ “KSK rollover" *had not been updated* to match changes made in 2022 to the DNS zones published, as a result of changing to new registry software (the IRS). And the InternetNZ technical procedure for performing DNSSEC KSK rollovers had similarly not been updated to specify longer gaps between the rollover steps were required. This resulted in timing critical “DNSSEC KSK Rollover” steps happening earlier than it was safe for those steps to happen in the new operating environment.

In addition the reviewers would like to record that CIRA (the Canadian Internet Registry Authority) went above and beyond their registry platform support contract requirements in providing assistance with a rapid “post incident review” of the identified causes and helping to validate the safe next steps that the InternetNZ .nz Operations Team could take to (a) complete the in-progress DNSSEC “KSK Rollover” maintenance tasks safely, and (b) defer, until a more complete analysis had been done, any further DNSSEC “KSK Rollover” maintenance tasks.

Related Documents

InternetNZ internal technical reports

Interested technical readers are referred to the internal status report (written contemporaneously with the event), and the internal technical incident report (completed a few weeks later), for additional technical detail:

- status.internet.nz.nz: DNSSEC chain validation issue for .nz (updated 2023-05-29 to 2023-06-01; plus a later link to the Incident report linked below)
- DNSSEC chain validation issue: technical incident report (published 2023-06-26)
- DNSSEC Practice Statement (of the .nz TLD and second level domains, published 2017-07-17)

We agree with the summary of events and conclusions of the internal report, and adopt that report as part of the basis for this external review of the Incident. Only detail directly relevant to this external review is repeated in this report, which is written for a more general audience than the internal technical incident report.

InternetNZ news and articles

General audience announcements published by InternetNZ surrounding the Incident:

- DNSSEC chain validation issue for .nz domains (published 2023-05-30)
- DNSSEC chain validation issue for .nz domains: updates (published 2023-06-01)

Known media articles about the Incident

- NZ websites down – Security update causes widespread internet outagesSecurity update causes widespread outages to NZ websites, apps (Newstalk ZB, published 2023-05-30 09:32)
- InternetNZ apologises for security mishap disrupting access to many .nz websites (Stuff, published 2023-05-30 15:17)
- Widespread website, app outages: InternetNZ apologises for ‘change of house keys’ gone haywire (NZ Herald, published 2023-05-30 17:27)

Other online discussion of the Incident

- Calling time on DNSSEC: The costs exceed the benefits (Matt Brown, posted 2023-06-02)
- Major DNSSEC Outages and Validation Failures (cumulative list, 2010 to 2023)
- GeekZone Discussion Thread for .nz DNS resolution issues (thread started 2023-05-30)

External review Terms of Reference

- Internet ".nz Chain Validation Incident Terms of Reference" (PDF)

Technical Context for Incident and Review Report

This is a deeply technical incident, which occurred at the boundary of two technical systems, one of which had been updated, and one of which *should have* had its configuration updated as a result, as outlined in the Incident summary. To fully understand the Incident causes in detail some background on DNS and DNSSEC is essential; technical readers who understood the summary in deep detail may wish to only skim read the next couple of sections.

The Domain Name System (DNS)

The Internet Domain Name System (DNS) is an Internet feature roughly equivalent to the contacts database in a modern smart phone: when a user wants to contact an Internet resource, their computer requests a look up in the DNS to translate the user friendly name of the service, that the user gave them, into a number the computer can use to actually establish the connection.

Even in 1983 (when the DNS was created), the "contacts database" for the Internet had grown too big to be practically maintained in *single* contacts database. So the DNS is a planetary scale, distributed, "contacts database" built from very many cooperating pieces. There has been a lot of evolution of the DNS technology in the last 40 years, and this summary only touches on some of the points relevant to this incident.

Some of the relevant pieces of DNS technology are:

- **authoritative DNS servers**: these hold the *definitive records for a portion of the contacts database*. For redundancy and resiliency there are usually at least 2, and often up to about a dozen authoritative DNS servers which hold the same definitive records for the portion of the contacts database. They are constantly answering questions from other computers on the Internet about their portion of the definitive records. There are many millions of authoritative DNS servers around the world, with different subsets of the "contacts database" relevant to them.
- **DNS registry**: each DNS registry maintains a list of "if you want to find out about a DNS name ending with, eg, .nz, then you should ask these computers for that information", and publishes these through DNS servers which constantly hand out "try asking here" suggestions. There are hundreds of DNS registries around the world. Usually the DNS registry has (almost) no authoritative DNS information to hand out; only "I would start here" hints.
- **recursive DNS servers**: recursive DNS servers are *your ever helpful friend* who you contact when you do not have someone's contact details in *your* smartphone contacts database, who you know always says "leave it with me, I will get back to you with the answer in a moment". Recursive DNS servers (usually) do not have any authoritative information stored locally. But they do have a few "start here" notes, and a lot of willingness to keep asking questions of other DNS servers until the track down an authoritative DNS server which can give them a definitive answer to pass on to the computer that originally requested it. There are many millions of recursive DNS servers around the world (usually distinct from the authoritative DNS servers).

Starting from scratch, a DNS lookup for something like "www.example.com", involves multiple questions to multiple DNS servers – all handled behind the scenes by your helpful friend, the recursive DNS server. When the recursive DNS server starts up, all it knows is a small table of

“root DNS servers”, which are (usually) hard coded into the recursive DNS server software. When the recursive server asks one of those root servers about “www.example.com”, they give it the hint “try asking one of the gtld-servers.net DNS servers”. When the recursive DNS server picks, eg, j.gtld-servers.net, and asks them about “www.example.com” it receives the answer “try asking one of a.iana-servers.net or b.iana-servers.net”. Then the recursive DNS server can ask, eg, a.iana-servers.net where to contact “www.example.com”, get the answer it was first after, and return triumphant to the computer friend that asked with the answer in the first place. (Technical readers will note this is a simplified example; among other things there is an entire side quest of “where do I contact a.iana-servers.net anyway” omitted.)

These chains of recursive lookups can be a lot longer, depending on the domain name involved, and also whether the “QNAME minimisation” DNS feature is used. “QNAME minimisation” avoids blurting out “ultimately I need the answer for ...” to *every DNS server contacted* (potentially leaking private information), and instead just sends the part of the name the recursive DNS server guesses is relevant to the query to that DNS server, which can lead to receiving a redirect back to the same set of authoritative DNS servers to ask a more detailed question. The use, or lack of use, of the QNAME minimisation feature is particularly relevant to resolving names in a .nz second level domain, as the DNS servers listed for both the .nz TLD *and* the .nz second level domains are the same (ns1.dns.net.nz to ns7.dns.net.nz): if the full name is included on the first query then the answer will be more immediately helpful than if the first query from the recursive server just asks “who should I ask about .co.nz names”.

Caching in the Domain Name System (DNS)

Even from these simple examples it is obvious that starting from scratch every time would lead to a lot of repeated requests, especially to the root servers: asking “where do I even start to find answers for a .nz name” to the root servers for every single DNS lookup would overwhelm the root servers almost immediately, and slow everything down. The same problem exists for every DNS registry server too – their “I would start here” answer is relevant to every query for the part of the DNS they manage, and they too would be quickly overwhelmed in constant requests for the same information. Request load is a (smaller or greater) problem for every authoritative server on the Internet, depending on how popular it is to look up their DNS records.

From the beginning the Domain Name System had an overload mitigation feature built in: recursive servers were encouraged to cache answers that they had received, so that they did not have to *constantly* ask the same questions over and over again, and instead your helpful friend the recursive server could refer to notes they made (in their cache) and either pull off the “TV chef” reveal of “here is an answer I prepared earlier”, or at least skip directly to the final step (“I know exactly who to ask about that, one sec”). In practice the “TV chef reveal” (a pre-prepared, cached answer) is the most frequent outcome. Which is fortunate as it dramatically reduces the load on the global DNS system to have *caching* recursive DNS servers quickly handling most of the workload.

Introducing caching into any technical system creates a new problem: how long can we rely on the cached information, looked up earlier, to still be accurate, and use it without any verification it is still current. Obviously it is *probably* still valid after a few seconds, and pretty unlikely to be *guaranteed* to be valid after a year. There’s a lot of time range between 5 second and 31536000

seconds (approximately a year), and the right "definitely will not change within N seconds" value varies from DNS record to DNS record, depending on many factors.

The DNS solution to the problem of "how long to allow the record to be cached" is that *every answer* comes with a TTL ("Time to Live") value, that indicates how many seconds the answer can be *trusted to still be current information* before it should be looked up again. Caching recursive DNS servers keep track of these TTL values received, and (effectively) deduct one second from them for every second, so they know when to discard them and request a fresh copy of the information. These "TTL" values form a contract between the authoritative DNS server ("definitely good for N seconds") and the recursive DNS server, and the DNS protocol expects the caching recursive server to rely on information being current for as long as the TTL expects it should be, without asking again, to reduce the load on the authoritative DNS servers.

As outlined in the Incident summary the exact value of TTL values on different TTL records played a big part in the 29-30 May 2023 incident; but to fully understand the Incident there's another key piece of DNS technology.

Domain Name Security Extensions (DNSSEC)

The Domain Name Security Extensions were added to the DNS protocol starting about 20 years ago (ie, they are around half the age of the core DNS protocol). DNSSEC was added to provide a way to verify answers returned by DNS servers more than the "trust me, its legit, would I lie to you" basis on which the entire early Internet operated on. At the time DNSSEC was created (in the early 2000s) there very much was a problem with DNS servers lying, often for commercial reasons – for instance giving an answer that pointed at a different server than the original one, which wrapped advertising around the service the user originally wanted. Or with DNS queries – which historically were always sent in clear text over the Internet – being intercepted, and a false answer returned in a way that the requester could not tell it was a fake answer.

To provide a way to verify the answers returned by DNS servers, an entire parallel set of DNS records can be added to the authoritative DNS servers *and* to the DNS registry servers, which provide sufficient evidence to confirm that "you can trust this answer because...". The DNSSEC information is as partitioned up as the authoritative DNS information, with each authoritative DNS server having only its local pieces of the DNSSEC keys and answers, that it can hand out – on request – along side the substantive DNS information requested. Verifying the DNS answers via DNSSEC thus requires collecting enough matching pieces to build a *chain of trust* from the root DNS server answer to the answers from the ultimate authoritative DNS server, and verify each answer along the way.

The DNSSEC extensions are optional for authoritative servers, but their use has been encouraged over the last 15 years.

The DNSSEC extensions are effectively mandatory for DNS *registries* (like the InternetNZ .nz DNS registry), because *without the DNS registry participating in DNSSEC there would be a gap in the trust chain* from the root servers to the ultimate authoritative server, making the feature useless to the authoritative DNS servers with names under that portion of the DNS (eg, under .nz). As a result, over the last 10-15 years almost all major DNS registries have deployed the DNSSEC

features, to facilitate their customers (domain name registrants) effectively using the DNSSEC features.

The relevant parts of the DNSSEC extensions to this incident are:

- the “Key Signing Key” (KSK) which has a function similar to a corporate seal, which is kept in a safe and brought out only occasionally to endorse certain important statements
- the “Zone Signing Key” (ZSK) which has a function similar to a special pen and ink used for official statements: used regularly, but only for this particular function, so if something is confirmed to be “written with this pen” then it can be trusted as a legitimate statement
- the “DNSKEY” record(s), which provide sufficient information about the KSK (corporate seal) and ZSK (“special pen”) to enable confirming a given record could only have been written involving that key. These DNSKEY records are stored along side the answers they authenticate in the authoritative DNS servers.
- the “DS” record(s), which provide “here’s how you can recognise the corporate seal you should expect from this server” hints, to validate an answer, given out along side the “if you want to know about that domain, ask these servers” hints. Most frequently these DS records are stored in the DNS registry systems.

It is possible to combine the DNSSEC KSK and ZSK functionality into one key – a really special pen that produces unique marks, that you tell everyone how to recognise directly – which is called a “Combined Signing Key” (CSK). That can work for small, lower trust, authoritative DNS servers. But especially for DNS registries the tension between “you need the key frequently to sign DNS records” and “you need to keep the key very secure” makes a combined signing key operationally impractical. So DNS registries, like the InternetNZ .nz DNS registry, use the split KSK and ZSK key approach for operational convenience – the KSK can be “kept very secure”, the ZSK is kept closer to hand for day to day use, and the KSK and ZSK can be changed at different times based on their risk of being compromised.

With DNSEC signing in effect, *every record* in the DNS zone will have a companion DNSSEC record – the “RRSIG” record – which is a “resource record” signature that can be used, once the correct keys have been identified (and verified), to verify a specific answer record being checked.

Validating the DNSSEC answers probably sounds like a lot of work – and it is – but fortunately once again your friend the recursive DNS server has your back: a *validating* caching recursive DNS server is the conscientious friend who wants to be certain they are only giving you accurate truthful answers and whenever they can they will ask for and verify the DNSSEC records, without troubling you with the details, of what and how they checked, unless you specifically ask for them.

Not all (caching) recursive DNS servers are configured to be *validating* caching recursive DNS servers: checking the DNSSEC values is an optional feature, and the recursive DNS server can choose just to take it on faith everyone tells it the truth. Enabling the DNSSEC validation features in caching recursive DNS servers, where available, has been encouraged for the last 10-15 years. So *validating* caching recursive DNS servers are commonly deployed, but definitely not universally deployed. Validating caching recursive DNS servers are widely deployed in Aotearoa | New Zealand.

Obviously adding *yet more* DNS records that need to be queried to get an answer would add a bunch of extra workload, to all DNS servers involved, if we did not allow the recursive DNS servers to pull the same "here's one I prepared early" TV chef trick as with the other DNS records. So every DNSSEC record ("DNSKEY", "DS", "RRSIG") also comes with its own TTL ("Time to Live") value which indicates how long the recursive DNS server can rely on those DNSSEC answers being *everything it needs to know* to validate DNS answers with DNSSEC. The validating caching recursive DNS servers can also cache the "I already checked, this information is legit for N more seconds" results as they find them, or the "the result was bogus last I checked and I have been told that will not improve for N seconds" outcome, and return those answers without further checking.

Foreshadowing: the TTL ("Time to Live") values and the caching of DNSSEC ("DS", "DNSKEY") records – for different amounts of time – turns out to be critical to understanding the Incident that occurred 29-30 May 2023.

InternetNZ and the .nz DNS registry

InternetNZ | Ipurangi Aotearoa ("Internet New Zealand Incorporated"), through its wholly owned subsidiaries, and more recently directly, has run the DNS registry for the .nz Country Code Top Level Domain ("CCTLD"), for over 25 years. The registry function was initially run through Domainz (a combined registry and registrar, with some third party registrars) from 1997 to 2002, and then through NZRS Ltd (the New Zealand Registry Services company, "NZRS"; a pure registry with only third party registrars) from 2002 to 2018; both subsidiaries were, at the relevant times, 100% owned by InternetNZ (the registrar functionality of Domainz was later sold off; NZRS was wound up after the registry functions were merged into the InternetNZ parent).

Since 2018 the .nz DNS registry functionality has been operated directly by InternetNZ staff, through its in house ".nz Operations Team".

Starting with NZRS the .nz registry was operated using the SRS ("Shared Registry System") a piece of software commissioned by NZRS, and developed in New Zealand. While there was originally an intention that the SRS software could be used by other DNS registries – it was even made open source (announcement; source code from 2011-03-29) – ultimately the SRS software was pretty much only ever used by the .nz DNS registry.

Between 2019 and 2022 InternetNZ selected and deployed new DNS registry software, aiming to be more compatible with the modern international DNS registry practices that had emerged over the past 20 years. The resulting IRS ("InternetNZ Registry System") platform was deployed into production on 2022-11-01, approximately 6 months before the 29-30 May 2023 DNSSEC chain validation incident.

The new IRS was based on the CIRA Registry Platform ("FURY") sold by the Canadian Internet Registry Authority (CIRA). Configuration and integration of the CIRA registry platform for the InternetNZ .nz DNS registry platform was done by the InternetNZ .nz Operations Team, and some Aotearoa | New Zealand third party IT consultants, with support from CIRA, throughout 2022.

Structure of the .nz “Country Code” top level domain

Historically the .nz DNS TLD only allowed end user registration under second level subdomains (eg, co.nz, net.nz, org.nz, etc). Some of these second level subdomains were allowed open registration, and others were moderated second level domains (eg, govt.nz) where prior approval was required to register a name in that second level domain.

In 2013 the .nz Domain Name Commissioner announced a change of rules to permit direct registration into the .nz TLD (2013-10-11), and direct registration into the .nz TLD was possible from 2014 (initially subject to transitional rules to benefit existing .nz registrations who previously had been forced to register under a second level subdomain).

All the historical second level domains have been retained (eg, co.nz, org.nz, govt.nz) and as those domain names were well established as part of organisation branding, and widely referenced, many organisations have continued to use the names registered under the .nz second level domains as their primary domain name. Open registration into second level domains that historically allowed open registration is also still permitted, and continues to be used in parallel with direct registration into the .nz top level domain. In particularly registration into the .co.nz second level domain is still heavily used, as it is still widely recognised by the general public.

Foreshadowing: the presence and importance of these .nz second level domains plays a big part in the 29-30 May 2023 Incident. Particularly due to the InternetNZ .nz registry operating *both* the .nz TLD zone *and* the .nz second level domains (eg, co.nz, org.nz), and using DNSSEC signing on both sets of DNS zones.

Readers interested in the extended history of the .nz DNS registry may wish to start with the Wikipedia page for the .nz TLD and the resources linked from there.

The .nz DNS registry and DNSSEC

Both the Domainz Registry System (“DRS”) and the original SRS (“Shared Registry System”) operated by NZRS pre-dated the invention of the Domain Name Security Extensions (DNSSEC).

DNSSEC registry functionality was added the .nz DNS registry starting in May 2011 (DNSSEC support in .nz), and the .nz TLD and the .nz second level zones have been fully signed since 2012.

There has been only one other, much more minor, issue with the .nz DNSSEC support, during the initial deployment phase – the formatting of the DNSKEY records were subtly incorrect in some cases, leading some (but not all) validators to be unable to validate them (DNSSEC for .nz, status update posted to the NZNOG mailing list, 2011-12-14).

Other than that minor very early implementation issue, InternetNZ (through its subsidiaries and directly) has operated the DNSSEC signing functions of the .nz DNS registry without any incident for over 10 years leading up to the 29-30 May 2023 DNSSEC Chain Validation Incident reviewed in this report.

We are also unaware of any other .nz DNS publication issues, that would have caused wide spread issues resolving .nz DNS names, occurring at any point in the 25 years that InternetNZ has operated the .nz DNS registry.

The 29-30 May 2023 Incident stands out as the unique incident with (partial) impact on resolving .nz DNS names, where the cause originated with the InternetNZ operated functionality.

DNSSEC signing in the .nz DNS registry

InternetNZ (originally through NZRS, directly through the .nz Operations Team since 2018) operates two sets of DNSSEC signing infrastructure, for redundancy. This DNSSEC signing infrastructure is used to sign both the .nz TLD zone *and* the 14 .nz second level domains into which end user registry is permitted for historical reasons.

The DNSSEC configuration of the .nz TLD zone signing, and the DNSSEC configuration of the .nz second level domain signing, is separate from both (a) the IRS .nz registry platform and (b) each other. Foreshadowing: this separation of the DNSSEC signing from the registry platform plays a significant role in the cause of the 29-30 May 2023 DNSSEC chain validation Incident being reviewed.

In summary, the current (since 2022-11-01) InternetNZ DNSSEC signing infrastructure has:

- two DNSSEC "signer" servers, in different data centres in different cities, each of which runs OpenDNSSEC for DNSSEC signing the .nz TLD and .nz second level domains, in parallel; each signer has a HSM ("Hardware Security Module") for managing the keys used for DNSSEC signing
- each DNSEC "signer" is configured with its own KSK ("Key Signing Key") and its own ZSK ("Zone Signing Key"), *for each of the .nz TLD and each second level domain*, with the private keys stored in its local HSM
- the KSK ("Key Signing Key") records for each DNSSEC signer (active *and* standby) are included in the "DS" records published in the DNS (so the standby is kept "ready to go")
- each DNSSEC "signer" is informed of the KSK and ZSK of the other signing server, so the published DNS information always includes the public parts of *both* the active KSK / ZSK keys *and* the standby KSK / ZSK keys, for each zone, in the DNSKEY records
- each DNSSEC "signer" server takes a feed of the DNS zones from the active IRS (registry) server, containing all the records registered in the .nz DNS registry, broken up into a .nz TLD zone, and separate DNS zones for each .nz second level domain, and creates signed versions of those DNS zones
- there are two hidden primary DNS servers, which are the intermediary between the DNSSEC "signer" servers and the public .nz DNS servers (ns1.dns.net.nz to ns7.dns.net.nz)
- at any time, both hidden primary DNS servers are configured to point at a single DNSSEC "signer" server, which is the active server; the other DNSSEC "signer" server runs continuously in the background, but its results are ignored until needed (the "standby" DNSSEC signer)
- all the .nz DNS servers (ns1.dns.net.nz to ns7.dns.net.nz) fetch DNS zone information from *both* (hidden) primary DNS servers, both of which are fetching from the same DNSSEC signer server

Prior to 2022-11-01 (and the production cutover to the IRS), the configuration for the SRS registry was similar, except that instead of the (SRS) registry directly providing the DNS zones the SRS

registry system would output a precursor data file containing the registry active information and a separate program would be run to build the DNS zones to be retrieved by the DNSSEC "signer" servers.

Foreshadowing: in the old (SRS) registry setup, the "DNS zone build" program would integrate the DNSSEC "DS" records pointing at the .nz second level domains as part of the *separate* DNS zone build, which could (and did from 2014) give the "DS" records a custom TTL value. But in the new (IRS) registry setup this "DNS zone build" functionality was directly part of the CIRA Registry Platform and the separate "DNS zone build" program was eliminated.

Foreshadowing: the new IRS platform required an additional program to ensure that the DNSEC "DS" records pointing at the .nz second level domains were injected into the IRS registry .nz TLD zone, in a manner equivalent to an end user registrant providing the "DS" record information along with their registration.

Technical readers may wish to note that (per the .nz DNSSEC Practice Statement of 2017-07-17):

- The current KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits;
- The current ZSK key pair(s) is an RSA key pair, with a modulus size of 1024 bits;

and following common DNS registry operational practice the KSK keys have the SEP ("Security Entry Point") bit set in the DNSKEY records, and the ZSK keys do not have the SEP bit set. Since there are always at least four DNSKEYs present (active/standby KSK, active/standby ZSK; six DNSKEYs during key rollover), the differences in key length and whether the SEP bit is set help identifying which keys are intended for which purpose when reviewing DNSSEC answers or, eg, DNSViz diagrams.

DNSSEC Key "rollover"

Like all security keys (and other secrets like passwords), best practice is to change them periodically to mitigate the risk that someone else might have discovered, or guessed, the private part of the key. Changing the security keys used for DNSSEC "signing" is called a DNSSEC Key "rollover".

Exactly how frequently to change ("rollover") the security keys used for DNSSEC is a matter of operational choice.

As described in the .nz DNSSEC Practice Statement (2017-07-17), the choices that InternetNZ made were:

- ZSK ("Zone Signing Keys"), which are shorter (1024 bit) and more heavily used, are changed every 3 months; and
- KSK ("Key Signing Keys"), which are longer (2048 bit) and have a much more specific use (signing ZSK key identities), are changed every year

These choices of rollover periods have been in place since InternetNZ (via its NZRS subsidiary) first deployed DNSSEC signing of the .nz TLD and second level subdomains (.co.nz, .net.nz, etc).

ZSK ("Zone Signing Key") rollover requires only changes within the zone being signed, and as a result the rollover of the ZSK can be fully automated by the OpenDNSSEC software:

OpenDNSSEC can keep track of when the next ZSK rollover is due for that zone, makes sure the correct timing is followed for each rollover step, and carries out the rollover tasks automatically. InternetNZ have the ZSK configured for "ManualRollover", which means *starting* the ZSK is a manual step (at a timing of their choice), but OpenDNSSEC can automate the other steps in the ZSK rollover.

KSK ("Key Signing Key") rollover requires *both* changes in the parent zone (to update the "DS" record in the parent key that indicates which keys are expected to be in use) *and* changes in the zone being signed. As a result the process of changing a KSK is only semi-automated in OpenDNSSEC.

Changing the KSK for the .nz TLD requires submitting a DS record update to IANA (through the root zone request ticket system), and waiting for that to be applied before carrying on with other steps.

Changing the KSK for a .nz second level domain is more automated, as in this case InternetNZ directly controls *both* the DNS records for the parent zone (.nz) *and* the DNS records for the zone whose KSK is being changed (eg, .ac.nz, .co.nz, .net.nz, etc). This potentially allows the semi-automated steps to be carried out with fewer built in delays waiting on external parties.

Because of the information caching in the DNS, described above, there is an inherent delay between when the DNSSEC "DS" and DNSSEC "DNSKEY" records are changed in the registry, and when you can be *certain* that *every recursive DNS server* **must have** realised that the older copy they had cached – without the new information just updated – was now out of date, and they have to fetch a new copy in order to carry on. These "how long to wait" values come from from the TTL ("Time To Live") records of the "DS" records (in the parent zone) and the "DNSKEY" records (in the main zone). Once enough time has passed that one can be sure that the TTLs have expired even on older copies of the records fetched seconds before they were changed, then it is safe to carry on with the next steps of the key rollover.

For a KSK rollover, which is semi-automated by OpenDNSSEC, the high level process is:

- a .nz Operations Team member starts the KSK rollover process for the relevant DNS zone, by running an OpenDNSSEC command, which associates a new KSK with the zone, and adds it into the "DNSKEY" records of the zone
- the .nz Operations Team member runs a command to retrieve the set of "DS" records for the zone being changed that OpenDNSSEC expects now to be present as a result of the update
- the .nz Operations Team member then takes steps to update the "DS" records pointing at the zone being changed in its parent zone (eg, if the KSK for .ac.nz is being changed they would update the "DS" records in the .nz zone that point at ac.nz to have the new records, by running an InternetNZ developed tool which injects those new "DS" records into the registry for the next DNS zone export; if the KSK for the .nz TLD itself is being changed, they would submit the new records in a "please update" request to the IANA root zone service)
- (some time later) the .nz Operations Team member verifies that the correct new "DS" records are externally visible in the parent DNS zone (ie, they are "visible now, for new requests")

- once the updated “DS” records are visible to new requests, the .nz Operations Team member informs the OpenDNSSEC software that the “update DS records in parent zone” is completed, by running a command that marks the KSK as “seen” in the DS records
- when OpenDNSSEC is informed the updated DS records have been seen it starts a timer, *based on a value in its configuration file for the DNS zone being changed*, which waits until OpenDNSSEC believes (*based on its configuration*) that *every* recursive DNS server *must have realised* there is a new copy of the “DS” record available, and have (or will as soon as it needs it) fetch the new copy of the record
- after the new “DS” record is publicly visible, OpenDNSSEC automatically starts using the new KSK value in the DNSSEC “signing” process *in parallel with the old KSK value*, and starts a timer for stopping using the old KSK value (*based on the OpenDNSEC configured time to wait*)
- then after enough additional time has passed – the TTL of the DS records, *from the OpenDNSSEC configuration*, plus some margin – on the next run of “ods-enforcer”) OpenDNSSEC stops using the old KSK in signing the DNSKEY records of the zone being changed

At this point the DNSSEC KSK rollover process is effectively complete – the only usable trust chain that will work is via the *new* DNSSEC KSK (“corporate seal”) signing the (existing) ZSK record (“special pen”). That (existing) ZSK continues to sign the records in the zone (until a separate “ZSK rollover” happens at some later point).

Once the rollover process is complete the old reference to the old KSK can be removed from the “DS” records in the parent zone, and the old KSK can be removed from the “DNSKEY” records of the zone being changed.

Normally for operational tidiness the .nz Operations Team would do this cleanup fairly promptly. For example removing the old .nz second level domain (eg, ac.nz) key from the registry, with an InternetNZ written program, which removes the old “DS” record from the next .nz TLD DNS zone build. (Since changes to the IANA managed root servers requires a support ticket, it is not uncommon for those old DS records to be left for longer, eg, until there is a reason to make another change, rather than always creating a ticket just to remove the old DS record.)

The .nz DNS zones and DNSSEC KSK rollover

Careful readers of the sections above will have noted that there are:

- KSK and ZSKs for the active DNSSEC “signer” for the .nz top level domain
- KSK and ZSKs for the active DNSSEC “signer” for each of the 15 .nz second level domains (.ac.nz, .co.nz, etc)
- KSK and ZSKs for the standby DNSSEC “signer” for the .nz top level domain
- KSK and ZSKs for the standby DNSSEC “signer” for each of the 15 .nz second level domains (.ac.nz, .co.nz, etc)

which is a lot of keys to update.

As described above, the OpenDNSSEC software and the InternetNZ integration of it completely automated the rollover of the ZSK ("Zone Signing") keys, every 3 months, and this process just looked after itself.

For the rollover of the KSK ("Key Signing") keys, this was handled by some InternetNZ operational planned maintenance tasks. InternetNZ's practice was to:

- start the KSK rollover task for the .nz TLD *on the least recently rolled over DNSSEC signer* first, up to submitting the change request ticket to the IANA Root Servers process (since the "request ticket" takes a while to get processed by hand)
- start the KSK rollover tasks for the .nz second level zones (ac.nz, co.nz, etc) *on the least recently rolled over DNSSEC signer* next, and work through the steps of those rollovers on the expected time schedule
- finish up the rollover tasks for the .nz TLD *on the least recently rolled over DNSSEC signer* once the changes on IANA managed root servers were completed to allow the remaining steps to continued
- once all of the above *least recently changed DNSEC signer* steps were complete, a few days later carry on and repeat the same set of steps for the *other DNSSEC signer,* for each DNS zone (.nz TLD, and 15 second level zones), as a second phase of the annual "DNSSEC KSK rollover") maintenance (which by that point would be the least recently rolled over)

Depending on the timing of when the DNSSEC signer KSK values were last changed, and when the DNSSEC KSK active and standby signers were last swapped over, this could result in the active DNSSEC signer having its KSK rollover done first (as in May 2023), or the standby DNSSEC signer having its KSK rollover done first.

InternetNZ treated the entire process listed above (ie, changing the one set of KSK keys for .nz and 15 second level domains, then changing the other set of KSK keys for .nz and 15 second level domains) as a single annual maintenance tasks – the "DNSSEC KSK rollover" maintenance task.

The process described above was followed both in previous years, and also in 29-30 May 2023. With the exception that because of the issues encountered on 30 May 2023, the process was (a) initially paused so that the "DS" records pointing at the old KSK values would not be removed, then (b) the OpenDNSSEC tasks were all paused while the initial internal investigation was done, only to be carefully resumed once there was a clearer understanding of the issue; and (c) at the time of writing this report, only the active DNSSEC signer KSK values have been changed (changing the standby DNSSEC signer KSK keys, per the second half of the normal maintenance process, has been on hold pending the completion of the internal and external reviews so any new checks or steps can be introduced before they are completed).

DNSSEC "Trust Chains"

Validation of DNS information via DNSSEC relies on the notion of "trust chains". The *validating* (caching) recursive DNS server attempts to build a path from *something it already knows* (the public DNSSEC KSK for the root DNS zone) to the record that it is trying to validate. (The record

it is trying to validate might be the originally requested answer, or it might be a "side quest" on the way to fetching the originally requested answer.)

Since the DNSSEC trust boundaries are (usually) aligned with the DNS delegation boundaries, and operators of DNS registries generally use the KSK ("Key Signing Key") / ZSK ("Zone Signing Key") separation, typically validating a DNSSEC "trust chain" to a specific record, starting from the root involves:

- obtaining the ZSK in use by the root zone, and validating it is correctly signed by the KSK hard coded into the DNS server software;
- obtaining the "DS" record that points at the KSK(s) used top level domain (eg .nz) containing the record to be validated, and verifying that "DS" record is correctly signed by the ZSK in use by the root zone
- obtaining the "ZSK" for the top level domain (eg, .nz) containing the record to be validated, and validating that ZSK is correctly signed by a KSK record obtained from the root DNS servers (and validated in earlier steps)
- repeating the above steps for each level down of DNS delegation down to the record to be validated (these delegation steps are *typically* matching the "."s in the fully qualified domain name), at each step fetching the "DS" record from the parent indicating the next KSK to rely on, validating that KSK "DS" reference with the *parent's* ZSK, using that next level KSK to validate the next level ZSK, and so on
- once reaching the ultimate signed record, validating that record is correctly signed with the ZSK of the final zone, and thus – since everything else before it was trusted – the specific record can be trusted.

If the *validating* recursive DNS server can get all the way through this process, from start to finish, then the "trust chain" of multiple levels of KSK/ZSK pointing at KSK/ZSK, etc, up to the final answer record, is said to be complete.

Crucially, as described above, the validating *caching* recursive DNS server will make *extensive use of its DNS cache* as part of the "trust chain" validation steps above. Because otherwise it would be constantly refetching the same information, adding delay and putting unsustainable load on the DNS servers nearer the root of the DNS infrastructure.

If anything goes wrong with validating this DNSSEC "trust chain" – a missing link, something pointing at a record that no longer exists, or a "bad signature" – then the *validating* recursive DNS server will call the resulting answer "Bogus", and refuse to use it – returning a "SERVFAIL" back to the requesting DNS client ("sorry, it didn't work out").

Operational Context for Incident and Review Report

Organisational Restructure

InternetNZ has gone through a significant period of change over the past 4 years. In 2018 The New Zealand Registry Service ("NZRS") and the policy function of the Domain Name Commission ("DNC") merged into InternetNZ.

It is understood there was a significant period of adjustment which led to a structural change process between December 2021 and 2022. (Please refer to Appendix I which sets out the structure and purpose of each puni.)

Part of this restructure introduced a new puni | team with three new roles; Te Puni Whakawhanake Rawa | General Manager Customer and Product, and two direct reports, .nz Operations Manager and a Product Operations Lead.

According to the final organisational restructure decision document this puni is:

> "...responsible for ensuring our products meet the needs of our customers, even as their needs change. This puni continues to be responsible for understanding and putting the needs of our customers at the centre of our work, with .nz the primary focus.
>
> The difference between these decisions and the December proposal is that rather than this puni having executive ownership responsibility for .nz with a distributed team, the technical roles in the .nz team is now aggregated into this function to give this puni all of the primary components to lead .nz in one team.
>
> This decision means that our .nz activity is now able to work as one coordinated function, under single leadership that owns the strategy, goals and delivery we have for .nz and products in one place.
>
> In addition to this, this puni develops and implements our customer-centric product strategy, with an emphasis on .nz first, and manages our income-earning and public-good products as well as discerning and sharing customer insights."

Mimosa Project

Along with the structural change, InternetNZ was embarking on a significant project, the Mimosa Project. This project was set up to find replacement software for the DNS registry platform. Over 3 years this led to the replacement of the Shared Registry System ("SRS") software, custom written in New Zealand for InternetNZ, with the registry platform provided by the Canadian Internet Registry Authority ("CIRA"), which is used by multiple other DNS registries world wide. InternetNZ called their deployment of the replacement DNS registry platform the "IRS" (InternetNZ Registry System).

The Incident

Between 29 and 30 May 2023, InternetNZ ran their standard annual rollover of the DNSSEC "Key signing keys" ("KSK"). InternetNZ have been running these updates for over 10 years and has never had any issues. The difference this year was that the process was run with the new registry system, IRS. InternetNZ was not aware at the time, that the new IRS had slightly different outputs

compared to their old registry system which were not picked up during the testing and validation phase of the new platform and integration with the DNS System.[1] This resulted in a number of end users being unable to access .nz domains, meaning some people were unable to access particular websites and, in the case of some stakeholder employees, not able to log on to their own network.

It is acknowledged that there has never been a critical incident like this in well over twenty years. The incident was caused by a technical issue, however, there is always a human element to consider. For example, how did the organisation handle the issue? Did they follow an appropriate process? Was the team adequately resourced? Is there anything InternetNZ can do from a human resource perspective to prevent an incident like this happening again?

Although it was not necessary for us to review the organisational change process, or review how the Mimosa Project ran, it was important for us to take into consideration the impact these events had on staff and to consider if there were any organisational cultural concerns that may have contributed to the Incident.

There was nothing in the review to suggest these key events were a direct cause of the Incident, but there were some subtle factors which ***may*** have contributed to the Incident in terms of how the .nz Operations Team were resourced and how the Incident response was raised internally.

[1] See the internal InternetNZ report on the Incident, https://internetnz.nz/news-and-articles/dnssec-chain-validation-issue-for-nz-second-level-domain/

The DNSSEC Chain Validation Incident: 29-30 May 2023

All DNSSEC KSK rollover processes carried out on Monday 2023-05-29 (the start of the technical Incident) were consistent with the InternetNZ DNSSEC KSK rollover practices successfully used in previous years, including the commands run and the timing of when the commands were run. All the commands and timing of running the commands was also consistent with expectation of all members of the .nz Operations Team of InternetNZ, at the time the commands were carried out.

If the circumstances surrounding the DNSSEC KSK rollover had *not* changed – ultimately as a side effect of having changed registry software, and particularly the DNS "zone build" process associated with the registry, in November 2022 – then the entire DNSSEC KSK rollover procedure would have been exactly as smooth as previous years, and no incident would have occurred.

Unfortunately the circumstances surrounding the DNSSEC KSK rollover *had* in fact changed, in a subtle way, that the .nz Operations Team of InternetNZ did not realise affected the KSK rollover process, until after the Incident had occurred (and was well under way).

As described in the "Time Period Under Review" section in the Introduction, the timeline of the ac.nz KSK rollover incident and timeline of the other .nz second level domain rollover incidents overlap, and blended into each other. So the two initial technical phases of the Incident are described below in more detail, and then treated as two phases of a single incident and incident response for the purpose of this review.

In all cases, the new DNSSEC active signer KSK keys were generated on Friday 2023-05-26, and associated with the relevant .nz TLD and .nz second level zones on Friday 2023-05-26. This step was carried out without any issue, and had no impact on the Incident as it merely made the new KSK keys *available to be used* but did not start using them.

The ac.nz KSK rollover incident

Because:

- the 29-30 May 2023 DNSEC "KSK rollover" was the first time the otherwise well practiced ("BAU" – Business as Usual) annual maintenance process was being done since the new (IRS) registry software had been installed, and
- because converting over to that new registry software had required writing an additional automation tool (to add/remove "DS" records for the second level domains into the registry zone for the .nz top level zone)

the InternetNZ .nz Operations Team wanted to start one of the .nz second level domain KSK rollovers earlier in the day, so that they could monitor the entire process for that KSK rollover more carefully, and make sure the new steps interacting with the IRS registry to add/remove "DS" keys worked as expected.

The experienced .nz Operations Team member assigned to carry out the .nz KSK rollover process in 2023 chose "ac.nz" as the first second level zone to complete, because (a) it was one of the smaller second level zones in terms of number of registrations in the zone, and (b) it was alphabetically first in the list of second level zones.

On Monday 2023-05-29 at 08:35, the new KSK "DS" record for "ac.nz" was submitted to the IRS registry software, for inclusion in the next zone build.

After confirming that the new "DS" record for "ac.nz" was publicly visible, on 2023-05-29 at 09:18 two OpenDNSSEC commands were run to (a) notify OpenDNSSEC that the updated "DS" record for "ac.nz" was publicly visible, and (b) manually run the OpenDNSSEC key rollover task that updates the rollover state of in progress key changes. At this point the OpenDNSSEC countdown timer started for it being assumed to be safe to stop using the old "KSK" for "ac.nz" for signing the "ZSK" for "ac.nz".

Then early afternoon on Monday 2023-05-29, at 12:55, the experienced .nz Operations Team member noticed that multiple hours had passed – longer than the time called for in the InternetNZ KSK rollover standard operating procedure for .nz second level domains – and manually ran the OpenDNSSEC "ods-enforcer" key rollover tool again, so it could update its internal state.

The OpenDNSSEC key rollover tool recognised that multiple hours had past since the updated "DS" record for "ac.nz" had been seen, *much longer than its configured time to wait after the record update had been seen*, and it proceeded on to the next phase of the "ac.nz" KSK key rollover, which was to automatically stop using the old KSK key for signing the ZSK (zone signing key). From the next zone publication run, *only the new KSK was used* to sign the ZSK, which was in turn signing "ac.nz" records. This meant that the DNSSEC "trust chain" to reach the signed records in "ac.nz" now exclusively relied on trusting the new "ac.nz" KSK.

On Monday 2023-05-29 at 13:00 the "DS" record for the old "ac.nz" KSK was also removed from the registry, so it too would be omitted from the next .nz TLD DNS zone build, which happened minutes later.

As far as the InternetNZ .nz Operations Team were aware on the early afternoon of Monday 2023-05-29, the "ac.nz" KSK rollover procedure had been successfully completed, following the same procedures and timings they had used in previous years, and in all their tests "ac.nz" DNS names could be successfully resolved, including with DNSSEC validation.

With hindsight we know that this was *not true for everyone* attempting to use ac.nz DNS names on the afternoon of Monday 2023-05-29. But the InternetNZ .nz Operations Team were not aware of any reports of issues resulting from the "ac.nz" KSK rollover until Monday 2023-05-29 15:31, over two hours later.

The other .nz second level domains KSK rollover incident

Since the "ac.nz" "KSK rollover" *appeared* to have happened successfully, following the same process and timings as previous years, the integration steps with the new IRS registry software had worked as hoped, and no reports of problems had been received by early afternoon of Monday 2023-05-29, experienced .nz Operations Team member working on the KSK rollover processes carried on with the remaining .nz second level domain KSK rollovers that same afternoon. This started about 4.5 hours hours after the "ac.nz" KSK rollover step adding the "ac.nz" "DS" records. Which was about 4 hours later than the InternetNZ .nz Operations Team process for the procedure in previous years would have carried on with the other 2LDs.

Between Monday 2023-05-29 13:06 and 2023-05-29 13:12 the new “DS” records pointing at the new KSK keys for each of the remaining 14 .nz second level domains were added, via the IRS registry API, into the .nz top level domain zone, to be published in the next DNS zone build publication.

After verifying that the updated “DS” records for the remaining 14 .nz second level domains were now publicly visible (ie, the DNS zone build process had successfully run and published them), between Monday 2023-05-29 14:13 and 2023-05-29 14:37 the OpenDNSSEC tool was run for each of the .nz second level domains marking the updated DS records as “seen”. Then at 2023-05-29 14:37 the OpenDNSSEC key rollover task was manually run, which started the OpenDNSSEC configured countdown timers for the next (automatic) tasks in each KSK rollover process.

The manual steps for the KSK rollover for the remaining 14 .nz second level domains was now complete, by 2023-05-29 14:37.

Careful readers will note that this is still before 2023-05-29 15:31, when the first report of issues with resolving ac.nz DNS names was reported. That is *all* the .nz second level domains had their active signer “KSK rollover” process well under way *before* the first report (about “ac.nz”) DNS resolution issues arrived.

On Monday 2023-05-29 at 22:40 the nightly cron job for the OpenDNSSEC task which updates the state of key rollovers in progress (“ods-enforcer”) automatically ran. Since many more hours had passed than time configured for OpenDNSSEC to wait after the “DS” records for the remaining .nz second level domains had been “seen”, OpenDNSSEC “ods-enforcer”) automatically marked the old “KSK” key as no longer required for signing the “ZSK” (ie it concluded it was already safe to just use the new “KSK” for signing the “ZSK”, based on its outdated configuration). This update the state of all remaining .nz second level domains.

On Monday 2023-05-29 at 22:45 the first DNS zone build since the old KSK DNSKEY records had been removed ran, and updated DNS zones were published to the Internet. These updated .nz second level domains had only the new “KSK” signing the “ZSK”, making the DNSSEC trust chain entirely reliant on the new KSK.

The InternetNZ .nz Operations Team first became aware of users experiencing issues with resolving other .nz DNS names starting 2023-05-30 00:16. (The first report that we are aware of they could have seen at the time was 2023-05-29 23:59, about 15 minutes earlier; although we are aware of users who experienced problems earlier than that but did not report it to the InternetNZ .nz Operations Team at the time.)

Various users of .nz DNS names (but *not all* users of .nz DNS names) continued to experience DNS resolution issues through the morning of Tuesday 2023-05-30 until either (a) enough time passed that the recursive DNS servers they were using had automatically fetched updated information, or (b) an administrator of the recursive DNS server had manually encouraged the recursive DNS server to forget old cached information and start DNS resolution of .nz DNS names again with fresh information. The end user impact is discussed in more detail in the “User Impact” section below.

The .nz TLD KSK Rollover

The .nz TLD "KSK Rollover" also started on Friday 2023-05-26. Updated "DS" record information was submitted to the IANA root servers process on Friday 2023-05-26,. That updated information was added by Saturday 2023-05-27 09:30, and definitely publicly visible by Saturday 2023-05-27 11:31.

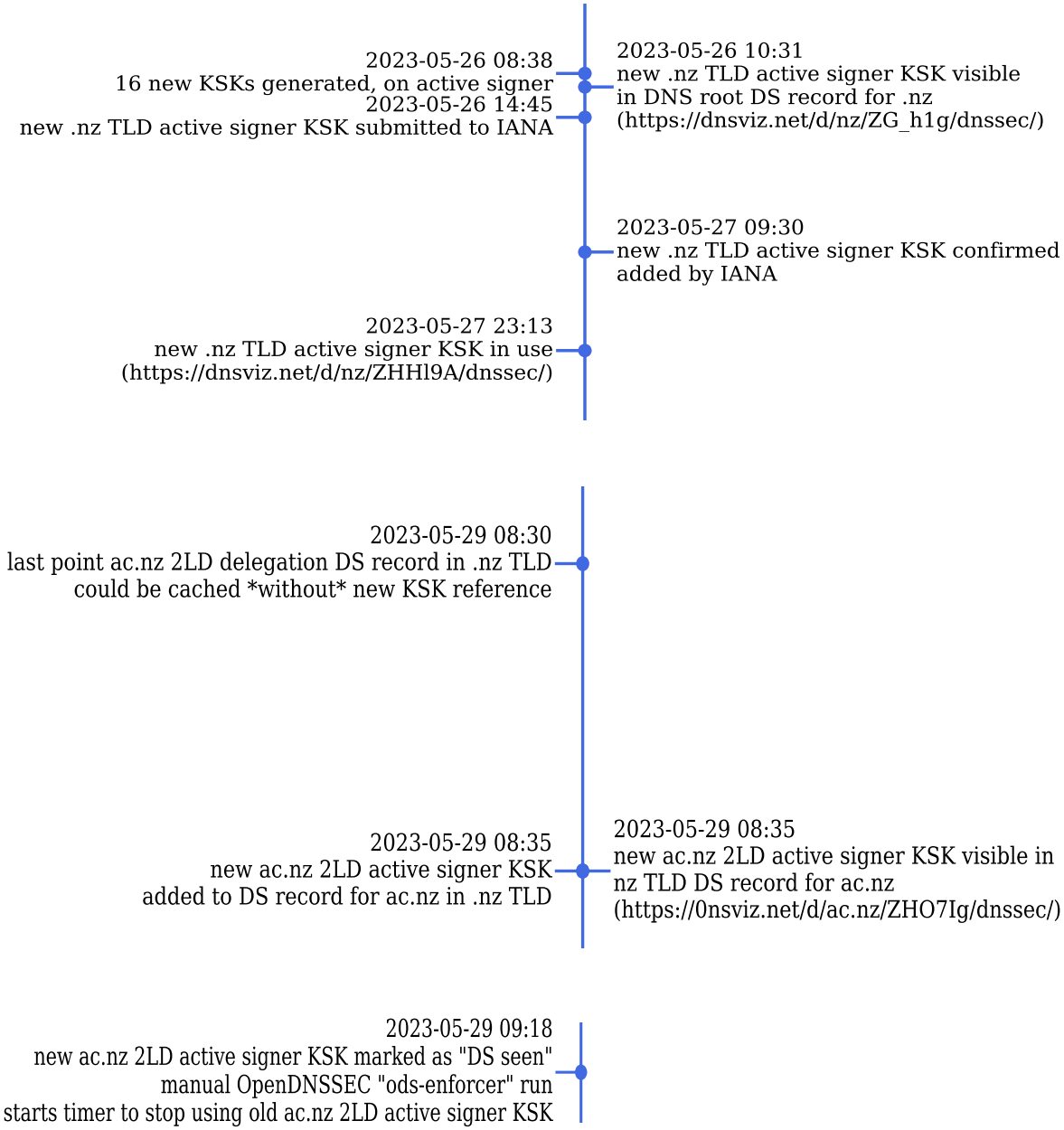
The new "DS" record for the .nz TLD was marked as "seen" on Monday 2023-05-29 12:55 (after the "ac.nz" DNSEC KSK Rollover had been done). Since that was at least 2 days after the "DS" record was *actually* publicly visible, plenty of time had been allowed in the .nz TLD KSK Rollover process.

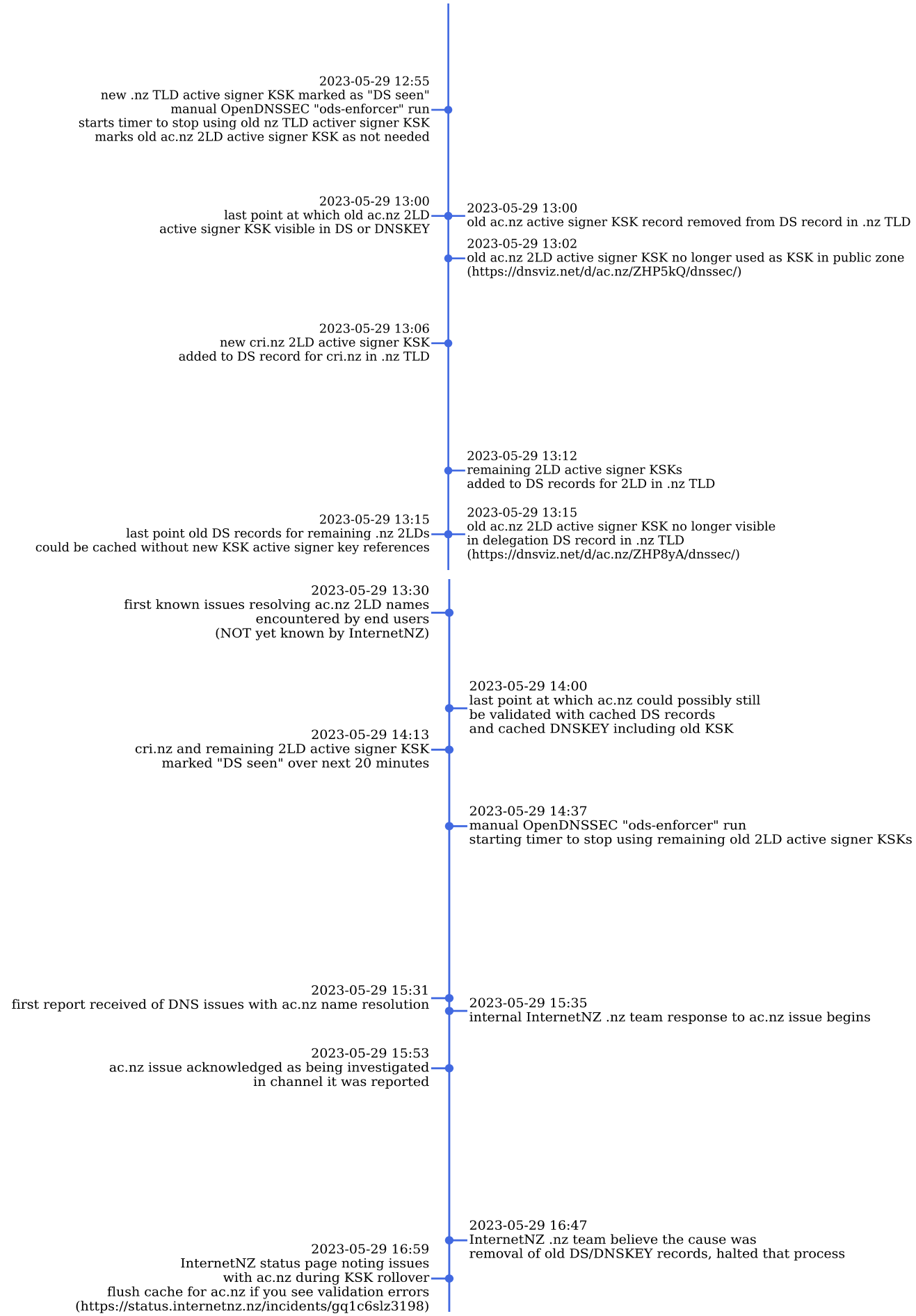
Since the .nz TLD DNSEC KSK Rollover process had OpenDNSSEC *correctly configured* to allow 1 day for the "DS" records to expire out of caches, and the OpenDNSSEC "ods-enforcer" process was suspended between 2023-05-29 22:40 (last automatic run) and 2023-06-01 15:51 (first manual run, to clean up after the Incident), the "DNSSEC KSK Rollover" process for the .nz TLD *itself* proceeded plenty slow enough for validating caches to detect the key transitions before they had to rely on them.

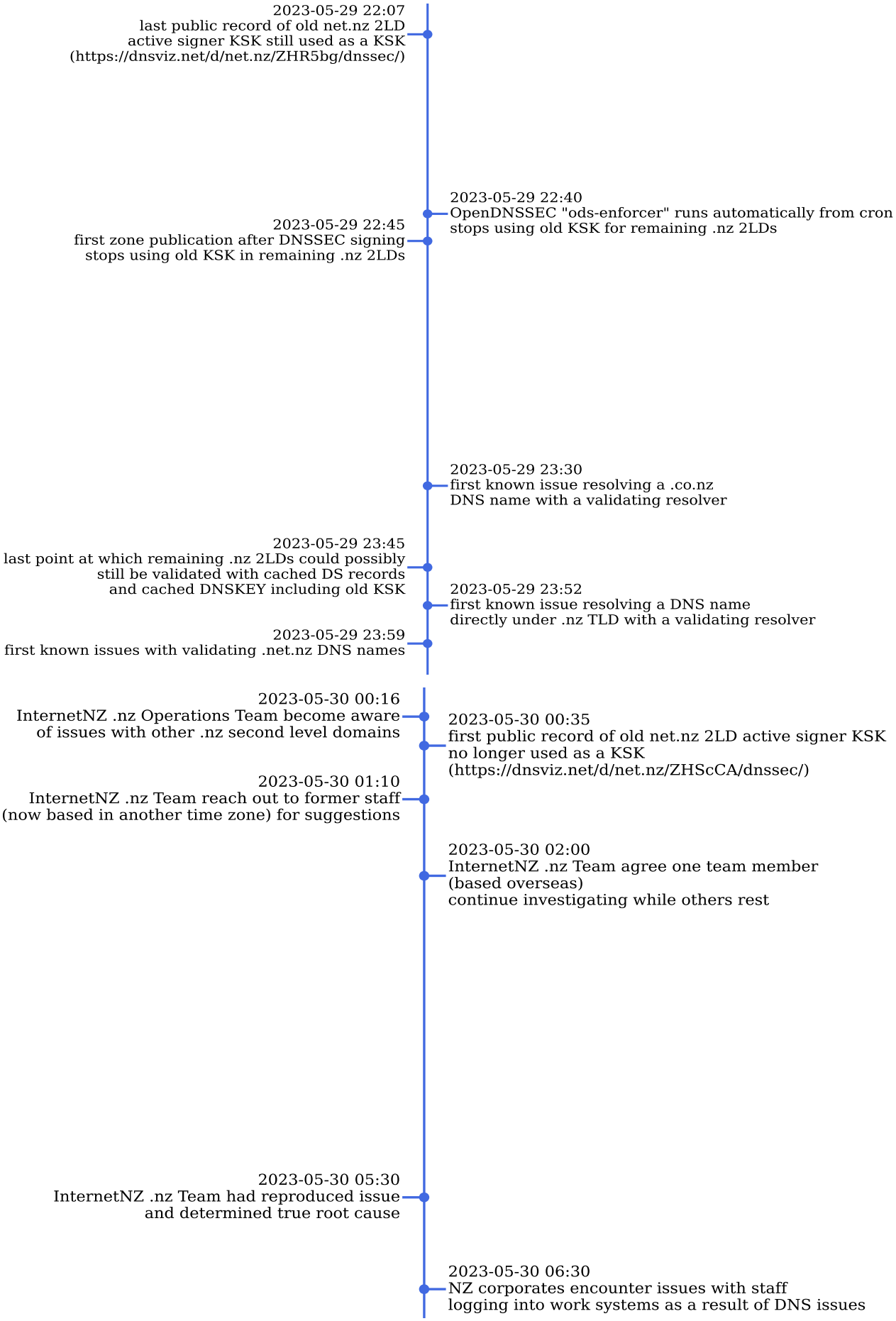
There were issues reported with DNSSEC validating resolvers validating DNS zones registered directly under the .nz TLD, but it is believed all those validating issues related to other resources that were part of the validation path (such as the DNS nameservers). This is discussed further in the "User Impact" section.

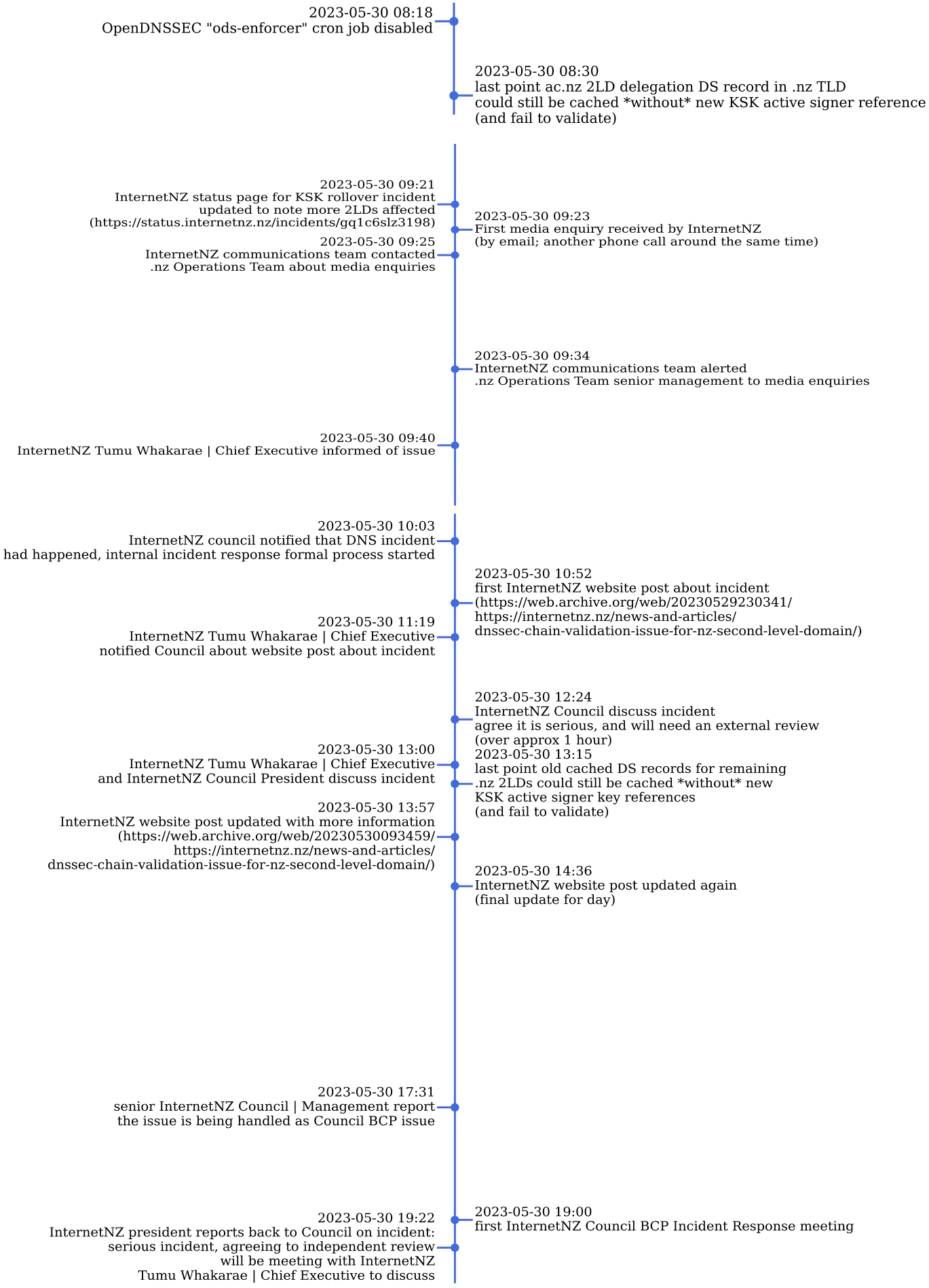
Detailed Incident Timeline

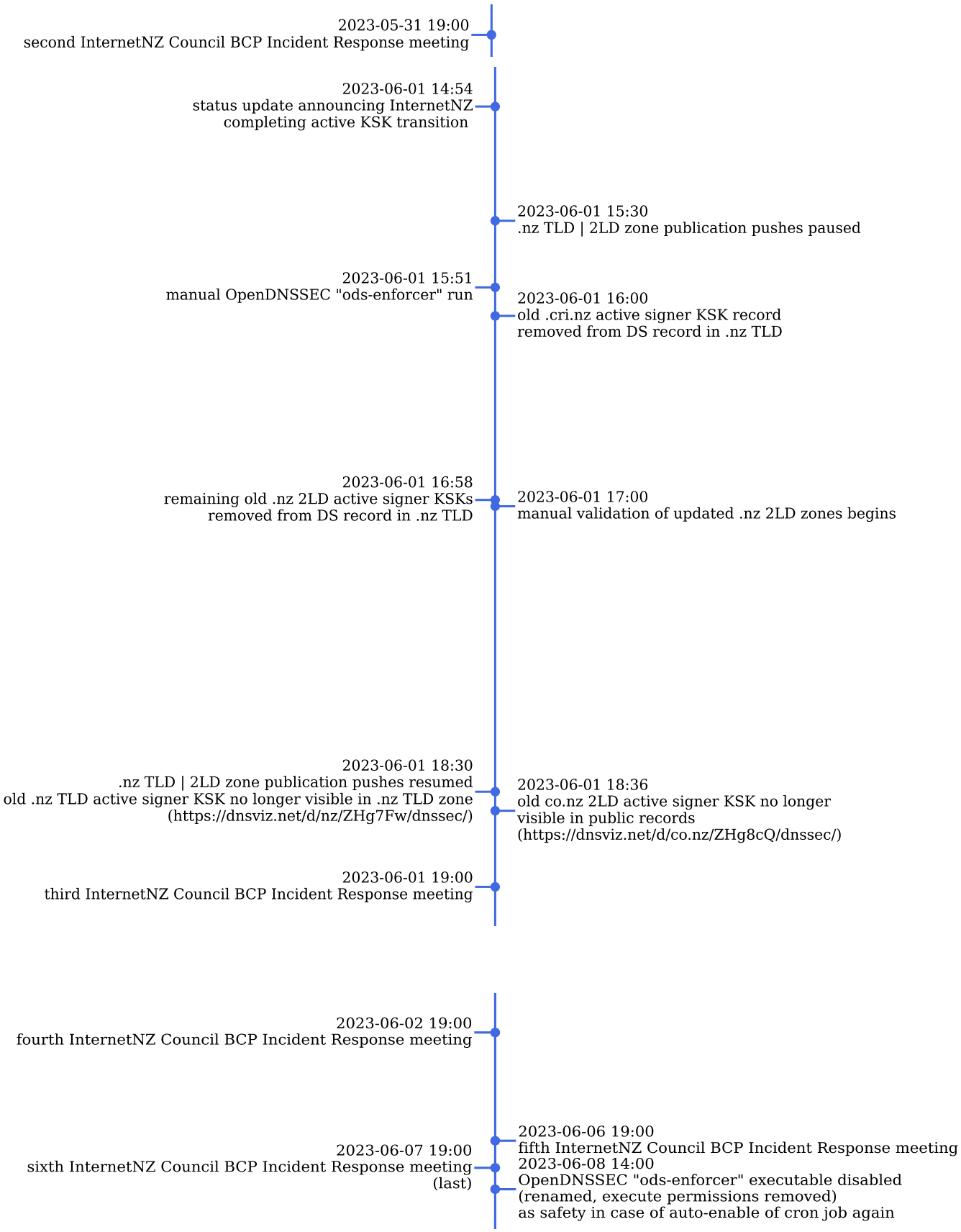
All timestamps are provided in Aotearoa | New Zealand local time at the time of the Incident (NZST, UTC+12). For readability this timeline has been divided up into sections of related events. Before and after the main Incident period these timeline periods cover multiple days; in the most active period of the Incident the timeline periods cover only a few hours, and in some cases parts of an hour. Readers are advised to refer to the timestamps provided with each event to determine relative gaps between events.




2023-05-29 12:55
new .nz TLD active signer KSK marked as "DS seen"
manual OpenDNSSEC "ods-enforcer" run
starts timer to stop using old nz TLD activer signer KSK
marks old ac.nz 2LD active signer KSK as not needed
2023-05-29 13:00
last point at which old ac.nz 2LD
active signer KSK visible in DS or DNSKEY
2023-05-29 13:00
old ac.nz active signer KSK record removed from DS record in .nz TLD
2023-05-29 13:02
old ac.nz 2LD active signer KSK no longer used as KSK in public zone
(https://dnsviz.net/d/ac.nz/ZHP5kQ/dnssec/)
2023-05-29 13:06
new cri.nz 2LD active signer KSK
added to DS record for cri.nz in .nz TLD
2023-05-29 13:12
remaining 2LD active signer KSKs
added to DS records for 2LD in .nz TLD
2023-05-29 13:15
last point old DS records for remaining .nz 2LDs
could be cached without new KSK active signer key references
2023-05-29 13:15
old ac.nz 2LD active signer KSK no longer visible
in delegation DS record in .nz TLD
(https://dnsviz.net/d/ac.nz/ZHP8yA/dnssec/)
2023-05-29 13:30
first known issues resolving ac.nz 2LD names
encountered by end users
(NOT yet known by InternetNZ)
2023-05-29 14:00
last point at which ac.nz could possibly still
be validated with cached DS records
and cached DNSKEY including old KSK
2023-05-29 14:13
cri.nz and remaining 2LD active signer KSK
marked "DS seen" over next 20 minutes
2023-05-29 14:37
manual OpenDNSSEC "ods-enforcer" run
starting timer to stop using remaining old 2LD active signer KSKs
2023-05-29 15:31
first report received of DNS issues with ac.nz name resolution
2023-05-29 15:35
internal InternetNZ .nz team response to ac.nz issue begins
2023-05-29 15:53
ac.nz issue acknowledged as being investigated
in channel it was reported
2023-05-29 16:47
InternetNZ .nz team believe the cause was
removal of old DS/DNSKEY records, halted that process
2023-05-29 16:59
InternetNZ status page noting issues
with ac.nz during KSK rollover
flush cache for ac.nz if you see validation errors
(https://status.internetnz.nz/incidents/gq1c6slz3198)


2023-05-29 22:07
last public record of old net.nz 2LD
active signer KSK still used as a KSK
(https://dnsviz.net/d/net.nz/ZHR5bg/dnssec/)
2023-05-29 22:40
OpenDNSSEC "ods-enforcer" runs automatically from cron
stops using old KSK for remaining .nz 2LDs
2023-05-29 22:45
first zone publication after DNSSEC signing
stops using old KSK in remaining .nz 2LDs
2023-05-29 23:30
first known issue resolving a .co.nz
DNS name with a validating resolver
2023-05-29 23:45
last point at which remaining .nz 2LDs could possibly
still be validated with cached DS records
and cached DNSKEY including old KSK
2023-05-29 23:52
first known issue resolving a DNS name
directly under .nz TLD with a validating resolver
2023-05-29 23:59
first known issues with validating .net.nz DNS names
2023-05-30 00:16
InternetNZ .nz Operations Team become aware
of issues with other .nz second level domains
2023-05-30 00:35
first public record of old net.nz 2LD active signer KSK
no longer used as a KSK
(https://dnsviz.net/d/net.nz/ZHScCA/dnssec/)
2023-05-30 01:10
InternetNZ .nz Team reach out to former staff
(now based in another time zone) for suggestions
2023-05-30 02:00
InternetNZ .nz Team agree one team member
(based overseas)
continue investigating while others rest
2023-05-30 05:30
InternetNZ .nz Team had reproduced issue
and determined true root cause
2023-05-30 06:30
NZ corporates encounter issues with staff
logging into work systems as a result of DNS issues


2023-05-30 08:18
OpenDNSSEC "ods-enforcer" cron job disabled
2023-05-30 08:30
last point ac.nz 2LD delegation DS record in .nz TLD
could still be cached *without* new KSK active signer reference
(and fail to validate)
2023-05-30 09:21
InternetNZ status page for KSK rollover incident
updated to note more 2LDs affected
(https://status.internetnz.nz/incidents/gq1c6slz3198)
2023-05-30 09:23
First media enquiry received by InternetNZ
(by email; another phone call around the same time)
2023-05-30 09:25
InternetNZ communications team contacted
.nz Operations Team about media enquiries
2023-05-30 09:34
InternetNZ communications team alerted
.nz Operations Team senior management to media enquiries
2023-05-30 09:40
InternetNZ Tumu Whakarae | Chief Executive informed of issue
2023-05-30 10:03
InternetNZ council notified that DNS incident
had happened, internal incident response formal process started
2023-05-30 10:52
first InternetNZ website post about incident
(https://web.archive.org/web/20230529230341/
https://internetnz.nz/news-and-articles/
dnssec-chain-validation-issue-for-nz-second-level-domain/)
2023-05-30 11:19
InternetNZ Tumu Whakarae | Chief Executive
notified Council about website post about incident
2023-05-30 12:24
InternetNZ Council discuss incident
agree it is serious, and will need an external review
(over approx 1 hour)
2023-05-30 13:00
InternetNZ Tumu Whakarae | Chief Executive
and InternetNZ Council President discuss incident
2023-05-30 13:15
last point old cached DS records for remaining
.nz 2LDs could still be cached *without* new
KSK active signer key references
(and fail to validate)
2023-05-30 13:57
InternetNZ website post updated with more information
(https://web.archive.org/web/20230530093459/
https://internetnz.nz/news-and-articles/
dnssec-chain-validation-issue-for-nz-second-level-domain/)
2023-05-30 14:36
InternetNZ website post updated again
(final update for day)
2023-05-30 17:31
senior InternetNZ Council | Management report
the issue is being handled as Council BCP issue
2023-05-30 19:00
first InternetNZ Council BCP Incident Response meeting
2023-05-30 19:22
InternetNZ president reports back to Council on incident:
serious incident, agreeing to independent review
will be meeting with InternetNZ
Tumu Whakarae | Chief Executive to discuss


2023-05-31 19:00
second InternetNZ Council BCP Incident Response meeting
2023-06-01 14:54
status update announcing InternetNZ
completing active KSK transition
2023-06-01 15:30
.nz TLD | 2LD zone publication pushes paused
2023-06-01 15:51
manual OpenDNSSEC "ods-enforcer" run
2023-06-01 16:00
old .cri.nz active signer KSK record
removed from DS record in .nz TLD
2023-06-01 16:58
remaining old .nz 2LD active signer KSKs
removed from DS record in .nz TLD
2023-06-01 17:00
manual validation of updated .nz 2LD zones begins
2023-06-01 18:30
.nz TLD | 2LD zone publication pushes resumed
old .nz TLD active signer KSK no longer visible in .nz TLD zone
(https://dnsviz.net/d/nz/ZHg7Fw/dnssec/)
2023-06-01 18:36
old co.nz 2LD active signer KSK no longer
visible in public records
(https://dnsviz.net/d/co.nz/ZHg8cQ/dnssec/)
2023-06-01 19:00
third InternetNZ Council BCP Incident Response meeting
2023-06-02 19:00
fourth InternetNZ Council BCP Incident Response meeting
2023-06-06 19:00
fifth InternetNZ Council BCP Incident Response meeting
2023-06-07 19:00
sixth InternetNZ Council BCP Incident Response meeting
(last)
2023-06-08 14:00
OpenDNSSEC "ods-enforcer" executable disabled
(renamed, execute permissions removed)
as safety in case of auto-enable of cron job again

InternetNZ response to the Incident

.nz Operations Team response

Monday 2023-05-29 into Tuesday 2023-05-30 morning

The InternetNZ .nz Operations Team first became aware of issues with the "ac.nz" DNSSEC KSK Rollover on Monday 2023-05-29 15:31. This was *after* the DNSSEC KSK Rollover for all the other .nz second level domains had already been completed to the point where automation (22:45 daily cron job) would finish the DNSSEC KSK Rollover *automatically*.

Three experienced .nz Operations Team members immediately started trying to identify what had gone wrong with the "ac.nz" DNSSEC KSK rollover that was causing *some* users to have problems resolving "ac.nz" names.

At this time the InternetNZ .nz Operations Team were unable to reproduce the problem themselves – their manual checks of authoritative records did not reproduce the problem, nor were they seeing the problem through validating recursive DNS servers they normally used (because t*he problem depended on a mix of older cached records and new records*).

The InternetNZ .nz Operations Team initial conclusion was that the *final step* of the "ac.nz" DNSSEC KSK rollover – removal of the old "DNSKEY" record for the old KSK – had been the cause of the "ac.nz" issue. So they stopped that process for the other .nz second level domains who had a DNSSEC KSK rollover in progress.

That conclusion was entirely plausible – prematurely removing the old KSK value from the "DNSKEY" record would cause the symptoms experienced. But unfortunately, with the benefit of hindsight, there was a second hidden cause – which also, by itself, could cause the same symptoms (OpenDNSSEC stopping signing the "ZSK" with the old "KSK" as it believes the old KSK is no longer needed).

In the case of "ac.nz" the two relevant steps occurred Monday 2023-05-29 12:55 (OpenDNSSEC "ods-enforcer" run that marks the old "ac.nz" KSK as no longer needing to be used), and Monday 2023-05-29 13:00 (script run that removed old "DS" / "DNSKEY" records).

So concluding that the "last step taken", which was a step that *could* cause the Incident, was *the* cause of the Incident was a reasonable initial conclusion. And it is unlikely any operations team, under real time pressure, would have identified there was a *second, hidden* additional cause.

As a result the initial conclusion of the .nz Operations Team was that the "ac.nz" issue was isolated to "ac.nz", and the other *already in progress* DNSSEC KSK Rollovers for the other second level domains should be successful. The InternetNZ "status" page for the Incident was started at this time, including the recommended step to mitigate the symptoms. And the initial conclusions reported back to the NZNOG Slack where the initial problem report had been received, with a pointer to that status information.

For this reason, and because of (a) the OpenDNSSEC signing of the zones known to be essential, and (b) an incomplete understanding of how the parts of the OpenDNSSEC software fitted together, the .nz Operations Team did not seriously consider disabling the OpenDNSSEC "ods-enforcer"

process on Monday 2023-05-29 evening. Which meant that ran automatically at 22:45, as it was scheduled every day, resulting in the wider Incident.

The three experienced .nz Operations Team members continued working on the problem well into the early hours of Tuesday 2023-05-30, particularly once they heard that there were also problems resolving other .nz second level domain names, starting late evening Monday 2023-05-30. They also attempted to reach out to other external support, including former .nz Operations Team staff, but unfortunately the time zones were not on their side to find experienced people available to help immediately (it was night in NZ/AU/US/CA).

Ultimately some of the team members left to get sleep (after having worked about 16 hours straight), and one other member carried on investigating possible causes.

That final team member managed to reproduce the wider validating DNS server lookup problem via an internal InternetNZ DNS server, analyse the records cached by that internal DNS server, and finally understand the *hidden additional cause*. This final diagnosis happened in the early hours of Tuesday 2023-05-30.

Once the true cause of the .nz problems were understood, it was clear that the DNS resolution issues had a fixed timeline before they would automatically resolve themselves (with the old "DS" cached records expiring out of the cache). And they knew that the process of expiring cached records could be accelerated by recursive DNS server operators if they encountered problems. So their conclusion was the safest approach was to avoid any potentially risky recovery steps, and focus on ensuring recursive DNS server operators knew how to identify and mitigate the issue.

Tuesday 2023-05-30

Once they understood the hidden root cause, the new current status of the "DNSSEC KSK Rollover" processes, and were able to check with external DNS experts that it was safe, the InternetNZ .nz Operations Team disabled the "ods-enforcer" cron job, so it would not run again until the reviews were completed.

For the remainder of Tuesday 2023-05-30 the .nz Operations Team assisted with the communication process (described further in the next section), did more retrospective analysis, and monitored the situation closely.

Thursday 2023-06-01

After preparing a procedure to complete the DNSSEC KSK rollover for the .nz second level domains, and having that planned procedure reviewed by external DNS experts, the InternetNZ .nz Operations Team completed the "DNSSEC KSK Rollover" process for the remaining .nz second level domains. By removing the old "DS" and "DNSKEY" records. At this point it was over 3 days since the new "KSK" started being used, so all caching validating recursive DNS servers had ample time to be aware of the new keys.

This final DNSSEC KSK Rollover process was accompanied by copious manual checking of the resulting DNS zones before they were published. It was completed without any issues report.

Thursday 2023-06-08

As an additional precaution, after the InternetNZ Council BCP process, and confirming with external DNS exports that it was safe, the InternetNZ .nz Operations Team disabled ("chmod 000") and renamed the OpenDNSSEC "ods-enforcer" binary to ensure that even if the "cron" configuration was restored by automation, the OpenDNSSEC "ods-enforcer" process could not run until the investigation process had been completed. It has remained disabled to this day, pending the outcome of the external review.

DNS server cache analysis is a "wicked problem"

We would like to record that one ISP helpfully provided a validating recursive DNS server "cache dump" which demonstrated the problem with resolving "ac.nz", to the InternetNZ .nz Operations Team, on the afternoon of Monday 2023-05-29. We have been able to confirm, through retrospective analysis with assistance from that ISP, that – among the many thousands of records in the cache dump – it does contain records demonstrating the hidden root cause. So with *perfect insight* the InternetNZ .nz Operations Team did have an example with which to identify "the" cause, but were unable to find it in the time available (ie, before Monday 2023-05-29 22:45 when the "ods-enforcer" cron job kicked off the second part of the Incident).

Analysing DNS cache dumps to determine a root cause of issues is:

- like looking for a needle in a haystack, the relevant records are a tiny subset of the records held in any production DNS server cache; and
- in this instance the .nz Operations Team needed to identify what records *were not in the DNS cache dump* but "should have been" if it were to operate normally (ie, the "DS" record pointing at the *new* KSK value)
- the analysis of DNS production cache dumps is most useful to validate (or invalidate) a theory about what you expect is the root cause (so as to narrow down what to look for)

In this case the production recursive DNS server cache dump was consistent with the first theory that the .nz Operations Team had for why the problem had occurred (the old KSK "DNSKEY" record has been "removed too soon"), as well as consistent with the *hidden cause* that the old KSK key was no longer being used to sign the "ZSK" and the old "DS" cached record did not contain the new "KSK" (that was now the only KSK key being used to sign the ZSK).

It is entirely understandable that the .nz Operations Team were not able to find the *second hidden cause* in real time in the DNS cache dump data, and realise in time to disable the "ods-enforcer" cron process that "the accident was already in progress" *and* that they still had a safe option to pause that DNSSEC KSK Rollover process for long enough that it would then be safe to continue.

That ISP production caching DNS server cache dump was invaluable for retrospective analysis and confirming the explanation in this report, and we thank them for making it available. (As far as we can tell they were the only DNS server operator with the foresight to keep a cache of the "broken state" that enabled this retrospective analysis.)

There is also a second respect in which "DNS server cache analysis" is a wicked problem, which is that if the investigator does not have a *live* DNS server which reproduces the problem – and the live

DNS servers they had access to did not exhibit the problem – then they are more limited in the tools they have available for analysis, and the resulting analysis is a much more manual analysis. It was ultimately only when one of the .nz Operations Team members found an affected internal validating recursive DNS server they could experiment with that they were able to narrow down the hidden cause of the Incident.

Wider InternetNZ response to the Incident

Were the right people notified of the Incident when it occurred?

InternetNZ Staff

The current Business Continuity Plan (BCP) focuses on responses relating to disasters such as earthquakes, fire or flooding, or security disasters such as computer crime or illegal entry into premises. There is a "Security Incident Detection and Response" guideline attached to the BCP which sets out an "incident" as defined as:

> "any irregular or adverse events that are significant or unusually persistent that occurs on any part of the InternetNZ core systems (SRS and DNS), networks and/or computers and meet one or more of the following criteria"

These criteria are related to computer security incidents:

- unauthorised access,
- malicious code,
- denial of service (DoS); and
- scans and probes

There is nothing that relates to full or partial outages due to technical errors.

However, the BCP does have a workflow diagram which indicates when .nz becomes unavailable, the InternetNZ Emergency Response Plan should be put in place. The issue was that only *some* .nz domains were unavailable to *some* users. The BCP response plan focuses on natural disasters, where it is likely all .nz domains would be unavailable rather than this type of Incident. Therefore, staff did not recognise that the BCP should have been activated at the time of the Incident.

The .ac.nz Incident took place (2023-05-29 15:31), and the .nz Operations Team thought they had the matter identified and resolved over an hour later. At that point they saw no reason to raise the Incident to senior management. By the time they were aware of the second phase of the Incident (2023-05-30 00:16), when .co.nz and other.nz domains could not be accessed, it became apparent the problem was more than first thought and was affecting more .nz domains.

Understandably .nz Operations Team was focusing on resolving the issue. By the time the second phase of Incident was identified, it was midnight. They did not think it was necessary to wake a member of the senior leadership team simply to give them a heads-up, particularly as they thought they would be able to identify and resolve the issue before most New Zealanders would be back at work the following morning.

It was only after the media contacted Internet NZ at around 09:23 on 2023-05-30 that others within InternetNZ became aware of the Incident. InternetNZ Communications contacted .nz Operations Team to advise they had received a media enquiry and asked what was happening. At that point it was recognised that the Incident was significant enough to raise with the GM at 09:34 and in particular, the CE at 09:40.

The CE took time to try and gather facts as to what had happened and then advised the Council at 10:03, letting them know she would be updating them once she had more information. At this point InternetNZ began an informal business continuity process.

In this case, the right people were notified and once notified, the appropriate steps were put in place in line with the BCP. The questions are whether the ***timing*** within which the senior leadership team was notified was appropriate and whether, if they had been notified earlier, a faster resolution of the Incident might have resulted?

The review showed some staff were unaware of the formal business continuity process. This is likely because there has been no critical incident like this in over 20 years and InternetNZ has gone through significant changes over the past four years. After reviewing the BCP, we believe it was likely, that those who were aware of it, did not identify this Incident as being significant because the BCP refers to an "incident" as being one that relates to an IT security which was not what this Incident was about.

Had it been clear that the Incident was significant enough to warrant raising the matter with the senior leadership team earlier, either at the 15:31 incident as a *"just to let you know this has happened but we think we have resolved the matter"* or 00:16 incident by sending an email to senior leadership saying *"this incident has happened and we are trying to resolve the matter"* or first thing the following morning on 30 May informing *"this incident has happened and we believe we know what the matter is and how it can be resolved"*, InternetNZ could have immediately stepped into the business continuity mode, even if just as a precautionary measure, and would have been ahead of the media. They would have been able to put a communication plan in place earlier to ensure a consistent message was given within the community. Having a clear explanation for "*why you are seeing these issues"* and ideally *"when things will be working again"* (by early afternoon 30 May at the latest) would have considerably reduced the concern of stakeholders as described in some of the media articles.

Once the Incident was raised internally, there was consistent feedback that the teams worked extremely well together while working through the plan and had a clear understanding of their roles and responsibilities. Based on the review, we would concur with that statement and commend the staff and the leadership team of InternetNZ for the way they handled the situation.

InternetNZ response to the wider community

InternetNZ was first made aware there was an issue via New Zealand Network Operators' Group ("NZNOG") Slack, an online community of network operators, predominantly in the internet and online services area. The group is intended to facilitate discussion among operators of networks in Aotearoa | New Zealand on matters relevant to network operators.[2]

.nz Operations Team used Slack to update the ISP community that they were in the process of identifying the issue. They also posted an update on the InternetNZ status on 2023-05-29 16:59 and 17:20 after the first incident ("ac.nz") was identified, with a recommendation of what to do should anyone encounter any issues.

[2] https://www.nznog.org

When the second phase of the Incident was identified (2023-05-30 00:11), .nz Operations Team, continued to use the NZNOG Slack to update the community but did not update the InternetNZ status until 2023-05-30 09:21, before they knew that the media had contacted the InternetNZ Communications Team.

The review only interviewed a small sample of external stakeholders/parties however, they provided consistent feedback.

- This was a significant Incident which impacted a number of people and businesses (see the "Impact on the Incident on End Users" section for more detail)
- The tone within the original communications both on the InternetNZ status page and on the website (original message published at 2023-05-30 10:52) left some feeling that InternetNZ was not taking responsibility of the fault and instead placing the fault on internet service providers ("ISP").
- The ongoing, updated communications that went out after noon were received positively and InternetNZ's using different communications channels ie NZNOG with links to the InternetNZ website to ensure there was a consistent message, was useful.

When asked what could have been done differently, the feedback was the same: it would have been good practice for InternetNZ to advise they were running an annual rollover of DNSSEC keys, particularly as it was the first time it was being run with the new IRS. This may have given stakeholders an indication that the issues they were experiencing might have been related to the rollover.

Impact of Incident on Internet users

Registrants and End Users

A name system like the DNS has two groups of users:

- holders of DNS names somewhere under the .nz top level domain ("registrants" in DNS terminology)
- end users *accessing* Internet resources via a name under the .nz top level domain

The first group ("registrants") were not *directly* affected by this DNSSEC Chain Validation Incident, as the DNS registry functions continued operating, and the DNS information continued being published.

But registrants of names under the .nz top level domain were affected *indirectly* in two ways:

- most registrants are also end users of their own DNS names under the .nz top level domain (for instance their staff using those DNS names to access company resources), *and* most registrants follow the Internet Best Practice guidelines of consuming their own DNS resources via a chain of DNS lookups that include the .nz registry DNS servers (that ensures what they see internally matches what their external end users see as well)
- most registrants have registered their DNS names under .nz, *in order that* other third parties (customers, partner organisations, etc) can reach the things that they publish on the Internet, and end users being unable to reach those things on the Internet can cause indirect harm (eg, loss of sales, higher than normal phone calls for information that is normally available on a website, etc)

Since the impact on both registrants (indirectly) and end users (directly) has the same cause – inability to reach DNS names under the .nz top level domain for a period of time – is the same, the impact is analysed from the point of view of end users only.

Time period of Internet end user impact

Users accessing the Internet through *validating* recursive DNS servers (operated by their ISP, their company, or an "open" recursive DNS Server such as Google, CloudFlare, or IBM) *may* have experienced issues resolving:

- domain names ending in "ac.nz" between Monday 2023-05-29 13:00 and Tuesday 2023-05-30 08:30 (up to 19.5 hours);
- domain names ending in another .nz second level domain (co.nz, net.nz, etc) between Monday 2023-05-29 22:40 and Tuesday 2023-05-30 13:15 (up to 14.75 hours)
- other domain names ending in .nz (including those directly under the .nz TLD, such as "internetnz.nz") between Monday 2023-05-29 22:40 and Tuesday 2023-05-30 13:15 (up to 14.75 hours) in some more specialised situations (discussed further below)

Based on reports received we believe that the validating recursive DNS servers used by most users affected by the first "ac.nz" issue were either (a) restarted, or (b) had relevant portions of their DNS cache flushed, on the afternoon of Monday 2023-05-29. So that most of those validating recursive DNS servers would have resumed being able to validate the domain names ending in "ac.nz",

thanks to timely DNS operator mitigation steps, by early evening of Monday 2023-05-29. As a result we estimate that the main period of impact for validating of domain names ending in “ac.nz” was about 5-6 hours, from Monday 2023-05-29 13:00 to Monday 2023-05-29 18:00 or 19:00.

For the wider .nz second level domain part of the Incident (starting Monday 2023-05-29 22:45), which affected co.nz, net.nz, etc, and in some cases names directly under the .nz top level domain (that depended on something under an affected .nz second level domain), we believe that the validating recursive DNS servers used by most affected end users were either (a) restarted, or (b) had the relevant portions of their DNS cache flushed, on the morning of Tuesday 2023-05-30. So most of those validating recursive DNS servers would have been able to validate all DNS names under .nz by mid or late morning on Tuesday 2023-05-30.

This gives these two periods where end-user impact was *likely* to have been encountered:

- Monday 2023-05-29 13:00 to Monday 2023-05-29 18:00, for users trying to reach names ending in “ac.nz” (assuming timely DNS operator action mitigated the main impacts at some point in the afternoon); and
- Monday 2023-05-29 22:45 to Tuesday 2023-05-30 12:00, for users trying to reach names ending in “.nz”, particularly names ending in a .nz second level domain like “co.nz”, “net.nz”, etc (again assuming timely DNS operator action mitigated the main impacts at some point in the morning of Tuesday 2023-05-30).

Circumstances for an end user of .nz to be affected

To be affected during this issue an end user (or a computer operating automatically on behalf of the end user) would need to have:

- used a *validating* recursive DNS server
- to look up a domain name under .nz (particularly under one of the .nz second level domains like .co.nz)
- where the *validating* recursive DNS server had cached some older information (the “DS” record) and tried to use that along with newer information (the new “DNSKEY” record and “RRSIG” DNSSEC signatures)
- and found that the old information and the new information were inconsistent, so declared the new information to be “Bogus”

These elements are discussed in below.

End users using a validating recursive DNS server

The percentage of users accessing the Internet through (DNSSEC) *validating* recursive DNS servers in Aotearoa | New Zealand appears to be quite high – the APNIC “labs” DNSSEC measurement graph for Aotearoa | New Zealand puts the percentage of users in Aotearoa | New Zealand accessing the Internet at over 85% of Aotearoa | New Zealand users behind *validating* recursive DNS servers, in the April to June 2023 measurement period. This is substantially higher than the world wide average APNIC measured of around 30% of users, worldwide, behind DNSSEC validating resolvers as of 2023 (APNIC labs "To DNSSEC or Not" published 2023-02-21).

The APNIC labs team behind those APNIC measurements have confirmed, by private communication, that their DNSSEC validation tests (deployed via their user measurement platform, which leverages global online advertising placement platforms) is confirming that each browser instance measured (a) can fetch an item with a valid DNSSEC signature and trust chain, (b) cannot fetch an item with an invalid DNSSEC signature/trust chain, and (c) fetches DNSSEC records like the DNSKEY indicating it is performing validation. (All these tests are performed with unique DNS names, so caching cannot affect the measurements.) So this indicates the majority of users in Aotearoa | New Zealand have their computers *only* looking up DNS information through *validating* recursive DNS servers (ie, if DNSSEC validation fails, they will not be able to reach the destination at all).

In addition the majority of Aotearoa | New Zealand users use DNS servers located in their ISP or their own organisation, rather than relying on open recursive DNS servers (such as the ones run by Cloudflare, Google, etc). For this Incident this is important because it means that for the majority of users prompt action by their ISP, or the administrators of their corporate recursive DNS servers, did a lot to mitigate the potential impact of this Incident.

End users looking up a domain name under .nz

As noted in the introduction, domain names under the .nz top level domain are widely used by individuals, businesses, and government organisations in Aotearoa | New Zealand. And over the last 20 years most businesses and government functions have moved online. So it is extremely likely that most people in Aotearoa | New Zealand would have been accessing Internet resources with names under the .nz domain during the affected period.

There will have been Internet users *outside Aotearoa | New Zealand* attempting to use Internet resources with names under the .nz top level domain, who may also have been affected. For instance Aotearoa | New Zealand residents and citizens travelling at the time of the Incident, or tourists planning a trip, or other overseas partner organisations of Aotearoa | New Zealand organisations. It is very difficult to quantify how many overseas Internet users may have been accessing Internet resources with names under the .nz top level domain in the relevant period, but (a) it is expected to be a much smaller number than those within Aotearoa | New Zealand, and (b) overseas users are less likely to be behind a *validating* recursive DNS server (and thus less likely to encounter the issue). For this reason we only consider end users *within* Aotearoa | New Zealand below, while acknowledging it is at best a lower bound on the user impact.

Validating recursive DNS server had cached some older information

The most complicated factors to assess, especially retroactively, are:

- what portion of the validating recursive DNS servers had cached the older "DS" records which did not include a reference to the new KSK key; and
- how long the validating recursive DNS servers retained and relied on that old information, before it either (a) expired automatically, or (b) was flushed from the cache as a mitigation step taken by the recursive DNS server operators

For "ac.nz" given the 1 day (86400 second) TTL on the "DS" records, the fact the new "DS" information was not published until Monday 2023-05-29 08:30, and that it is very likely that *a user*

would have accessed an “ac.nz” name through any relevant validating recursive server *before* 08:30 (on Monday 2023-05-29) – triggering the caching of the old information for 24 hours – we think it is very likely that *most* recursive validating DNS servers had the old “DS” information cached for “ac.nz” at the time the old KSK stopped being used (Monday 2023-05-29 12:55). The only validating recursive DNS servers that would *not* have had the old “DS” records for “ac.nz” cached would be those that happened to expired their cached record in the Monday 2023-05-29 08:30 to Monday 2023-05-29 13:00 time frame, and been lucky enough to have fetched the *new* “DS” record in time. Since that’s a 4.5 hour window, assuming an equal distribution of access to the records, there is about a 20% chance of a validating recursive DNS server having fetched the new information in time to avoid seeing any problem, and an 80% chance it still only had the old information cached.

For the other .nz second level domains, and .nz top level domains impacted by the .nz second level domain issues, the overall time window of potential impact is:

- shorter (first possible impact is Monday 2023-05-29 22:45); and
- overnight in the Aotearoa | New Zealand time zone (so there are fewer users potentially affected at the start of the affected period, as there are fewer users active overnight)

The shorter period reduces the chances a given validating recursive DNS server still had the old “DS” information cached, and increases the chances the old information would have expired by itself (and thus been replaced with current information) before the end of the potential risk window. In particular the new “DS” information for the other .nz second level domains was published around Monday 2023-05-29 13:15, so only validating recursive DNS servers which cached the “DS” information before then would be affected. The records making it possible to rely on the old “DS” information were not removed until Monday 2023-05-29 22:45, which is 9.5 hours later. Again assuming an even distribution of access to the records, there was about a 40% chance a given DNS server had already fetched the new “DS” information in time, and was unaffected; and a 60% chance the validating DNS server saw some period of DNS resolution issues starting late evening Monday 2023-05-29.

End users experiencing failures due to inconsistent old and new DNS records

For “ac.nz” access we expect *most* validating recursive DNS servers of users accessing ac.nz names would have been affected on Monday 2023-05-29 afternoon, due to the short window (4.5 hours out of the 24 hours TTL) to have fetched the new information, and around an 80% chance the validating recursive DNS servers had the old “DS” information cached. But that timely mitigation actions by particularly Aotearoa | New Zealand ISPs would have largely mitigated that issue by the end of the Monday 2023-05-30 afternoon as far as most affected users were concerned.

Given the overnight nature of the timing of the other .nz second level domain KSK rollover Incident, we assess the main period of end user for this second phase of the impact as between about Tuesday 2023-05-30 06:00 (as users start waking up and perhaps starting their jobs or other tasks needing the Internet) and Tuesday 2023-05-30 12:00 (by the time almost all validating recursive DNS servers would have had mitigation measures applied if required).

By mid morning Tuesday 2023-05-30 particularly ISPs operating recursive DNS servers for their users were aware of the DNSSEC KSK rollover Incident, and were able to take actions to mitigate the impact of the Incident on their users. Since, as noted above, the majority of Aotearoa | New Zealand Internet users use the recursive validating DNS servers run by their ISPs, these actions by the ISP operators of recursive DNS servers would have mitigated the issue for most users.

For other DNS server operators (eg, of in-house DNS servers at larger organisations), the InternetNZ information and media attention coming out late morning Tuesday 2023-05-30 would have alerted them to steps they could take to mitigate the impact of the Incident, if they had not already taken action.

In addition since Tuesday 2023-05-30 06:00 to Tuesday 2023-05-30 12:00 falls towards the end of the 24 hour period where the old "DS" records could have been cached (for 24 hours from Monday 2023-05-29 13:15) we think it is likely that by late morning Tuesday 2023-05-30 many validating recursive servers would have "self healed" by automatically expiring the old cached "DS" records they fetched more than a day ago, and getting fresh information.

We have found some indications that *some* validating recursive DNS servers may *proactively* fetch new "DS" records when encountering a DNSSEC validation error – ie, discarding their cached record early to enable quicker recovery – but have not been able to confirm this auto-recovery feature in specific software or software versions. We think this type of auto-recovery from key rollover issues, if done in a manner that minimises the additional load on the global DNS servers – perhaps trying to fetch new information every 5-15 minutes – is a very good implementation feature to reduce the impact of mistakes like the InternetNZ .nz KSK rollover Incident. Such auto-recovery features are definitely not universally implemented in recursive DNS servers, and any similar "DNSSEC KSK rollover Incident" is still likely to require considerable manual mitigation steps by recursive DNS server operators.

Examples of end user impacts

To give some concrete context to the end user impacts, here as some examples of end users impacts we are aware of:

- Multiple universities received reports some of their staff and students could not access their "ac.nz" domains on the afternoon of Monday 2023-05-29, which would have interrupted university work for a period of time; these reports were escalated internally and/or to their ISPs
- Many ISPs reported being contacted on the afternoon of Monday 2023-05-29 about issues accessing only "ac.nz" domains, spent staff time attempting to debug why only "ac.nz" was affected, and eventually took steps to mitigate the issue (by flushing the DNS cache) without yet fully understanding *why* the issue had happened (because they did not know InternetNZ was doing a DNSSEC KSK rollover maintenance task for ac.nz that day)
- A user with DNSSEC signed ".nz" domain reported being unable to access their own domain, late evening on Monday 2023-05-29, leading them to stay up debugging the issue and ultimately restarting their recursive DNS server to restore service (without fully understanding why it happened until later)

- Multiple ISPs reported that their automatic monitoring systems suddenly started triggering with alerts for being unable to reach ".nz" resources in the late evening of Monday 2023-05-29, and they had to triage why they were getting sudden "false" alarms (eventually tracking it down to DNS resolution issues, and mitigated by flushing DNS caches)
- Multiple ISPs reported their recursive DNS servers under higher than normal query load, as a result of failed queries (clients will automatically retry (a) with every recursive DNS server they know about, and (b) soon afterwards if they did not get an answer the first time). One ISP reported going from near-zero "SERVFAIL" statuses on DNS queries before the Incident to around 100,000 "SERVFAIL" status *per minute*, starting around 2023-05-29 23:30 and that rate of "SERVFAIL" errors continuing until the daylight hours of Tuesday 2023-05-30. Because the validating recursive DNS servers were finding the new DNS information was "bogus" due to not matching the cached "DS" records.
- Multiple technical users reported issues in the early hours of Tuesday 2023-05-30 (Geekzone discussion thread) accessing .nz domain names (especially .co.nz domain names), and ended up taking self-help steps such as changing to another DNS server (eg switching from desktop to a mobile on 4G, or switching their recursive DNS server settings to CloudFlare).
- A large Aotearoa | New Zealand corporate (in a critical infrastructure industry) reported that starting from around Tuesday 2023-05-30 06:30 they were getting reports their staff could not log into work systems to start their work day, and it was unclear to them what was causing the issue (we believe this included staff working from home and staff working in the office)
- On Tuesday 2023-05-30 morning multiple users reported issues accessing websites with .nz domain names, including media services, banking services, and online shopping. Most of these reports are from before mid-morning Tuesday 2023-05-30.
- On Tuesday 2023-05-30 multiple users, and organisations, reported issues using apps (such as online banking apps, or media streaming apps) that used ".nz" domain names behind the scenes. Most of these reports are from before mid-morning Tuesday 2023-05-30.

Impacts for accessing domains directly under the .nz top level domain

Users accessing "ac.nz" domains on Monday 2023-05-29 and other .nz second level domains on Tuesday 2023-05-30 through a validating recursive DNS server were directly impacted by the caching effects of the DNSEC KSK rollover Incident.

But the DNSSEC KSK rollover of the .nz top level domain *itself* proceeded perfectly without incident. And yet users of domains directly in the .nz top level domain (eg, internetnz.nz) also reported problems.

We believe there were at least two ways that users of names in the .nz top level domain were indirectly impacted:

- one of the resources associated with that .nz domain was under a .nz second level domain, and the validating recursive DNS server ran into "bogus" results in the process of the "side quest" of finding out how to contact that other resource with, eg, a ".co.nz" name or a ".net.nz" name (eg a nameserver for the domain, or a webserver for the domain); or

- the validating recursive DNS server ended up on a side quest to find out how to contact the InternetNZ .nz DNS servers (ns1.dns.net.nz through ns7.dns.net.nz), and in the process of that side quest, tried to validate "net.nz" answer on the way to resolving, eg "ns1.dns.net.nz" ran into a "bogus" result for net.nz and then gave up.

The second situation – the side quest resolving, eg, .net.nz – could perhaps have happened due to the modern "QNAME minimisation" DNS feature where the validating DNS server would ask parts of its question at a time – "where do I find out about .nz names", "where do I find out about .net.nz names", etc – each time being directed to the "next" DNS server. In the case of asking about ".nz" names *and* asking about ".net.nz" names the DNS servers to contact are the same – ask one of ns1.dns.net.nz to ns7.dns.net.nz. But by asking the question repeatedly, there's a much higher chance that the *validating* recursive DNS server is going to try to validate that the delegation back to the same set of DNS server is *itself valid* and find a "bogus" answer. And then give up on the whole query.

Whereas a validating recursive DNS server *without* "QNAME minimisation" in use will blurt out the entire question all at once, and is very likely to get directed to the final nameservers for that "directly in .nz" domain name with the valid ".nz" DNSSEC signatures, and thus never embarked on the side quest of, eg, validating ".net.nz" in the first place. This is one possible downside, in the context of DNSSEC validation, of the privacy enhancing "QNAME minimisation" feature.

End users accessing DNS names *directly* under the .nz top level domain are *less likely* to have encountered issues accessing Internet resources via those .nz top level domain names than users accessing domain names under one of the .nz second level domains (eg, .co.nz) directly affected by the "DNSSEC KSK rollover" Incident. But we have confirmed reports of problems accessing DNS names directly under the .nz top level domain from late evening on Monday 2023-05-29, so it definitely did affect some users of names directly under the .nz top level domain.

Conclusion on user impact

Because the vast majority (around 85% -- End users using a validating recursive DNS server) of Aotearoa | New Zealand Internet users access the Internet via a *validating* recursive DNS server (often the one run by their ISP), it is likely that most Internet users in Aotearoa | New Zealand accessing the Internet during the first 10 hours of the wider .nz second level domains part of the incident experienced some impact from this .nz "DNSSEC KSK Rollover" Incident. Fortunately the majority of that first 10 hours was overnight in Aotearoa | New Zealand.

While the majority of these issues were resolved within a few hours as far as most affected users saw (due to the old inconsistent information either being expired from the DNS cache by, eg, their ISP, or expiring automatically due to age), many end users starting their day on Tuesday 2023-05-30 could have experienced a very confusing set of symptoms where their Internet connection "mostly worked" (they could access things based overseas without problems), but a collection of Internet resources relying on ".nz" domain names did not work. And yet potentially other people they knew had no problems (depending on the state of other DNS server caches).

In addition multiple ISPs spent time receiving error reports from their users, debugging the issues internally, and dealing with additional load on their DNS servers as a result of this Incident. At least until they either pinned the issue down to InternetNZ changes that made the DNS server cache

information outdated, or proactively restarted their DNS servers or flushed their DNS cache as a troubleshooting step.

Without the combination of (a) timely actions by the ISPs operating the recursive DNS servers used by most Aotearoa | New Zealand Internet users, and (b) the time of day the issues started (resulting in most users being asleep through a considerable portion of the affected period) this Incident could have had much wider end user impacts. If the issues accessing banking services, media services, and online shopping were not resolved by late morning Tuesday 2023-05-30 – enabling end users to complete these tasks in the afternoon – there could have been considerably more downstream impact from this InternetNZ .nz DNSSEC KSK rollover Incident.

Technical Incident Findings

"A system that performs a certain function or that operates in a certain way will continue to operate in that way regardless of the need or of changed conditions."
— John Gall "The Systems Bible", 3ed, General Systematics Press 2002 (p69)

"The crucial variables are discovered by accident."
— John Gall "The Systems Bible", 3ed, General Systematics Press 2002 (p76)

"Complicated systems produce complicated responses to problems."
— John Gall "The Systems Bible", 3ed, General Systematics Press 2002 (p153)

All computers and software involved in this Incident – operated by InternetNZ and others – *operated correctly according to the way they were configured* throughout this "DNSSEC KSK rollover" Incident.

All InternetNZ staff acted in the same manner any reasonable DNS registry professional would have operated, throughout the Incident. All relevant commands were correctly entered, in the correct order, and at an appropriate time based on the long established InternetNZ standard operating procedure for the task being carried out, which had successfully been used multiple previous years.

Technical "root causes"

The triggering event for third party validating caching recursive DNS servers declaring newly fetched DNSSEC signed records "bogus" was:

- still having an old cached "DS" record, which did not reference the new KSK; *and*
- fetching a new "DNSKEY" record which no longer contained the old KSK signing the existing ZSK as valid (only the new KSK signing the existing ZSK as valid)

Because the "DS" records had a 1 day (86400 seconds) TTL, and the "DNSKEY" records had a 1 hour (3600 seconds) TTL, it was very likely that a validating caching recursive DNS server would fetch the new "DNSKEY" record while it still had the old "DS" record cached. If it did so it would see that neither of the two KSK values it expected to be used (in the old record – the old active KSK, and the standby KSK) were used for signing in the newly fetched "DNSKEY" record. At the point the Incident occurred, *only* the new active KSK was being used for signing the ZSK, and the caching validating recursive DNS server did not know that it should be trusting that new KSK – so it did not trust the new KSK. Resulting in the DNS answers being declared "bogus".

The two "root causes" that triggered this Incident were:

- the configuration of the OpenDNSSEC "ods-enforcer" program had not been updated to reflect the changes to the "DS" TTL value as a result of replacing the DNS "zone build" process during the transition to the new ("IRS") registry system (so the "ods-enforcer" program did not wait long enough before moving on to it next step of stopping using the old KSK key); and
- the InternetNZ .nz Operations Team standard operating procedures for performing the annual "DNSSEC KSK Rollover" maintenance process had also not been updated to reflect the need to

wait longer between the steps, because of the changes to the "DS" TTL value as a result of replacing the old ("SRS") DNS "zone build" process with the new ("IRS") registry system

Following these well established processes, *in the face of changed condition*s – the new "DS" TTL values – meant that the results of following the well established processes were not what had happened previously, or what was expected to happen, but instead resulted in the Incident experienced due to the mismatch between the expected/configured "DS" TTL time and reality.

The relevant OpenDNSSEC configuration had been configured by the InternetNZ .nz Operations Team (and the equivalent team at NZRS, the former InternetNZ subsidiary, before them).

None of the configuration for OpenDNSSEC or the "DNSSEC signers" was provided by the Canadian Internet Registry Authority (CIRA) as part of the new registry platform.

The OpenDNSSEC configuration, and the entire "DNSSEC signer" platform, pre-dated the introduction of the new registry platform by many years, and had been known to be "due for replacement soon" for some time.

Due to time constraints a decision was made to deploy the new "IRS" registry platform (based on the CIRA "FURY" DNS registry system) using the existing InternetNZ OpenDNSEC "signer" servers, and for InternetNZ to build some integration features between the old OpenDNSSEC "signer" servers and the new IRS platform.

These new integration features – for adding and removing "DS" records and "DNSKEY" records – functioned correctly throughout the Incident. But especially on Monday 2023-05-29 this new integration between the old "DNSSEC signer" system and the new IRS registry system was the main "new thing" that the .nz Operations Team were concerned to verify operated correctly during the "DNSSEC KSK Rollover". So their focus was on checking something other than the "DS" TTL values during the initial phases of the "DNSSEC KSK Rollover".

Inconsistencies in OpenDNSSEC configured and public DNS "DS TTL"

The InternetNZ .nz Operations Team were aware that the new (IRS) registry platform applied "TTL" (time to live, ie safe to cache) times to DNS records differently to the old (SRS) registry platform. This came up both during the initial production deployment (when the TTL was found to be set to 7 days instead of the expected 1 day TTL on most records), as well as during the pre-production testing when the inability to have different TTL values on the "DS" records and other records was noted.

The inability to have different TTL values on the "DS" records and other records was also discussed with the registry platform vendor, CIRA, including in February 2023 (three months before the Incident). It is not a feature present in the CIRA "FURY" DNS registry platform at this time, and none of the other CIRA "FURY" registry platform users had previously had different TTL values set on different records. So the feature had not previously been considered for implementation in the "FURY" registry platform.

Unfortunately this awareness that the "DS TTL value is different in the DNS zones built by the new IRS registry" did not translate into a concrete set of steps that had to be undertaken before the next annual "DNSSEC KSK rollover" maintenance task was started.

It appears this general awareness of "different TTLs in the new registry" did not get adequately recorded as a "post Mimosa Project" (ie, new DNS registry platform deployment) task that had to be addressed before the next "DNSSEC KSK Rollover" annual maintenance process. The InternetNZ .nz Operations Team were also faced with other urgent technical work immediately after the IRS registry went into production (including urgently moving out of a data centre being closed earlier than previously advised by the supplier), which distracted attention from the DNS TTL issues.

There were no technical controls that prevented the "DNSSEC KSK rollover" task from being started without ensuring the OpenDNSSEC *configured* "DS TTL" value and the IRS registry exported "DS TTL" value were the same. So the risk of the inconsistency was overlooked when starting the "DNSSEC KSK rollover", and only discovered in hindsight.

This 2022/2023 inconsistency between the DNS registry platform "DS TTL" and the OpenDNSSEC *configured* "DS TTL" value was the *second time* that the "visible in the public DNS" "DS TTL" value had been different from the OpenDNSSEC configured "DS TTL".

There had also been inconsistent values in those two locations between:

- 2014-02-20 when the "DS" TTL in the public DNS was reduced from 1 day (86400 seconds) to 1 hour (3600 seconds), at the request of DNS registrars, to enable faster recovery from DNSSEC issues (a widely recommended approach; some sources recommend reducing the "DS" TTL below 1 hour – see, eg, DNS OARC 40 Lightning Talk: Reducing default DS TTLs for Faster Failure Recovery presented in February 2023)
- 2018-06-20 when the OpenDNSSEC "DS TTL" configured value was reduced from 1 day (86400 seconds) to 1 hour (3600 seconds), to match the value configured in the DNS zone builds.

So for a period of four years (from 2014-02-20 to 2018-06-20) the (at the time NZRS, subsidiary of InternetNZ) .nz Operations Team operated the OpenDNSSEC "signers" with a mismatched "DS TTL" configured value.

Fortunately between 2014 and 2018, the configured OpenDNSSEC "DS TTL" value was *longer* than the DS TTL in the public DNS. So the only impact was that between 2014 and 2018 the "DNSSEC KSK rollover" process *could have* safely happened faster. But doing the "DNSSEC KSK rollover" process slower is always safe – the timeline requirements are *minimum* times to wait, and (other than operational issues from larger DNS records) there are effectively no maximum safe time limits.

However this extended period – 4 years – where inconsistent configuration was present highlights that there were no automated systems which were preventing a "DNSSEC KSK rollover" from being started with inconsistent configuration, nor was there monitoring regularly reporting on the inconsistency in a way that constantly drew attention to the configuration mismatch.

Furthermore due in part to the multiple years of restructuring of InternetNZ / NZRS, and other staff turnover, relatively few of the InternetNZ .nz Operations Team had been on the team since 2014 or even 2018, which further reduced the chances of anyone on the .nz Operations Team remembering that mismatched values between the "DS TTL" value in the public DNS and the "DS TTL" value in the OpenDNSSEC configuration could occur. We believe this lack of continuity of "institutional

knowledge" slowed down the identification of the true root cause on the afternoon/evening of Monday 2023-05-29.

Two part Incident – "ac.nz" and other .nz second level domains

There were two separate, but highly related, DNSSEC KSK rollover incidents: the first for "ac.nz", and the second for the other .nz second level domains.

All the DNSSEC KSK rollovers for all the second level domains had been started, and the "timer countdown" in OpenDNSSEC – based on the now known to be incorrectly configured value – were underway for all the second level domains *before* any reports arrived of DNS resolution issues as a result of the first ("ac.nz") KSK rollover process.

This meant that the "accident was already in progress" by Monday 2023-05-29 15:31 when there was the first report received that anything had gone wrong. The InternetNZ .nz Operations Team did not *start* the other .nz second level domain "DNSSEC KSK rollover" tasks after receiving reports of the "ac.nz" issues; they had already been started.

The final piece of the "DNSSEC KSK rollover" Incident for the other .nz second level domains *happened automatically* when a long scheduled, daily, "cron" task ran the OpenDNSSEC "ods-enforcer" process automatically. Effectively detonating the bomb that had been unknowingly ignited in the early afternoon of Monday 2023-05-29 (13:15).

With the benefit of hindsight, the InternetNZ .nz Operations Team could have safely disabled the "ods-enforcer" cron process (which ran nightly at 22:45) indefinitely, to pause the "DNSSEC KSK Rollover" process for the other .nz second level domains, but:

- the InternetNZ .nz Operations Team did not know at the time that OpenDNSSEC marking the old KSK to no longer be used for signing the ZSK was the triggering step of the "ac.nz" Incident (as they had made other changes immediately after that, which reasonably seemed more likely to be the cause)
- the InternetNZ .nz Operations Team did not have as detailed an understanding of the roles of the individual OpenDNSSEC tools as they gained after the wider .nz second level domain KSK rollover Incident
- the InternetNZ .nz Operations Team were aware that parts of OpenDNSSEC had to keep running to keep publishing, and updating, DNSSEC signed DNS zones otherwise wider problems with DNS resolution would occur

So the InternetNZ .nz Operations Team did not seriously consider disabling the "ods-enforcer" "cron" job on Monday 2023-05-29. This specific point is discussed further below in the "opportunities missed" section, as it is the specific question most third party technical people spoken to during the review process had about the Incident: the "ac.nz" part of the Incident was "understandable, if unfortunate", but for it to then later affect the other .nz second level domains was surprising and in need of explanation.

The actions taken after the "ac.nz" issues were reported, to suspend the step of removing "DS" and "DNSKEY" records for the other second level domains, could reasonably have been expected to

avoid repeating the same problem for the other second level domains, based on the information available to the .nz Operations Team on the day.

In particular prematurely removing the “KSK” record from the .nz second level zone “DNSKEY” *would have caused exactly the problems experienced in this Incident*, and that was reasonably the first analysis of the InternetNZ .nz Operations Team for why the “ac.nz” Incident had occurred. That analysis guided the steps they took immediately after that incident, before the Incident also affected the other .nz second level domains.

Many other steps that the Internet .nz Operations Team might have taken (some of which are discussed below in the “opportunities missed” section) could reasonably have been believed to risk causing further harm, and thus were reasonably not considered as part of the immediate incident response.

There are, and the InternetNZ .nz Operations Team were aware of, many other cases where attempting to “do something to fix a DNSSEC issue” has caused a much larger issue, particularly as a result of taking another step with the wrong timing. So a reasonable, prudent, DNS registry operator is wise to proceed cautiously with technical remediation actions.

Delayed notification

Notification to the InternetNZ .nz Operations Team of issue with “ac.nz” were unnecessarily delayed because InternetNZ performed the “DNSSEC KSK Rollover” maintenance process without prior notice to the Aotearoa | New Zealand Internet community.

Valuable hours of feedback were lost (especially the two hours between 2023-05-29 13:30 and 2023-05-29 15:31) as operators of recursive DNS servers, especially at ISPs, tried to understand why they were suddenly seeing unexpected problems resolving “ac.nz” domain names. Those operators were forced to debug the issue from first principles, aware that “something” must have happened but not knowing what it was, or who it should be reported to until they managed to identify a clear inconsistency in their DNS caches.

If the Aotearoa | New Zealand DNS operators were aware in advance that InternetNZ was performing the *once a year* “DNSSEC KSK Rollover” process that same day it is likely they would have made the connection between the “strange symptoms” they were debugging and the possible cause of the DNSSEC KSK Rollover change (in hindsight known to be the cause). This would likely at least have caused one of them to ask “hey, we are seeing strange symptoms with ac.nz, do you think it is related to your maintenance task” much earlier – potentially two hours earlier.

If the notifications of problems with “ac.nz” had been received earlier, with more proximity to the “ac.nz” rollover steps, it is more likely that the exact steps performed in the last hour could have been examined in more detail, which might have lead to identifying the true root cause on Monday 2023-05-29. Instead of identifying the “last step taken” with ac.nz as the most likely root cause – given the reports did not arrive until hours after that step – and incorrectly concluding that avoiding doing that “last step” on the other .nz second level domains would have avoided any problems with those other second level domains (a reasonable conclusion, and a necessary step, but with hindsight an insufficient step on its own).

In addition if the “ac.nz” final steps – the “ods-enforcer” update to stop using the old KSK, and the “DS” / “DNSKEY” removal – had not happened in such close proximity (about 5 minutes apart), then it would have been more likely that the specific first trigger of the Incident (the “ods-enforcer” update) might have been identified earlier.

Any system involving an extensive amount of caching of “old” data is extremely vulnerable to delayed reporting of problems, as it can continue functioning after some critical breaking change for some period based entirely on the cached information. In this case it was not until the older “DNSKEY” records (1 hour TTL / 3600 seconds) expired, leaving behind only the older “DS” records (1 day TTL / 86400 seconds) to be compared with the *new* “DNSKEY” records, that the problem became visible *in affected validating caching recursive DNS servers*.

The partial viability of the problem state, depending on whether or not the validating recursive server had old cached information, also complicated identifying how wide spread the cause was, which delayed the response to the Incident as it was initially believed to be much smaller than it turned out to be.

Conclusions of Technical Incident Findings

During the technical review, we identified, and multiple people we spoke with for the review brought up, various “opportunities missed” to avoid the technical Incident, or particularly to avoid the spill over from the initial “ac.nz” technical Incident into the wider “all second level domains” technical Incident. We address many of those “opportunities missed” in the next section, along with our understanding for why those opportunities got missed.

Finally after discussing the opportunities missed we close with a summary of additional technical and technical process recommendations to reduce the risk of a similar “DNSSEC KSK rollover” Incident occurring again in the .nz top level domain, and to enable mitigating any similar incident much quicker.

Operational Incident Findings

Was there appropriate support for the .nz Operations Team when the Incident happened?

Feedback showed once the senior management team became aware of the Incident, the .nz Operations Team was appropriately supported.

The relevant GM was heading to the United States to attend a business meeting when he became aware of the Incident. A decision was made for him to continue with his travels and attend the meeting because staff from the CIRA, which is a key partner, would also be at the meeting. Should there be any need to connect with the CIRA over the Incident, there would be someone there to have those discussions face to face. Furthermore, the GM would be in a similar time zone to another .nz Operations Team member who is based overseas and be able to provide appropriate support for them.

Despite the GM being overseas, he was still able to provide appropriate support for the CE and attend every crisis management and slack meeting needed as well as provide advice to the CE when requested.

The CE was able to support the team in whatever way was needed while their manager was overseas which was positively received.

Was .nz Operations Team adequately resourced to handle the Incident?

The role

Currently there are 4 members in the .nz Operations Team, and a manager who are expected to be on a rotational 24/7 on call roster. They are not all specialists, and although it would be ideal to have two experts in different areas, it is not easy to recruit for these roles. One team member is located in a different time zone which allows them to work outside New Zealand business hours. This is beneficial as it allows team members to rest while another works on any issue that may arise outside New Zealand business hours.

Being a 24/7 on call team, means they are expected to be available and ready to acknowledge alerts within 30 minutes. This requires them to have a laptop and access to a reliable internet connection wherever they might be and requires them to maintain the ability to access to the .nz VPN to remotely investigate and resolve incidents.[3]

Even if staff are not on call, there may be times when engineering staff can be escalated to out of hours. Reasons could include being the subject matter expert, platform experience, physical distance from a fault, etc.

The scope of work

Four years ago, the scope of the work the team was doing was quite different. At that time, it was recognised and agreed they would have another 1 FTE. Then NZRS and the policy area of DNS were merged into InternetNZ which meant the recruitment of a new team member was put on hold. Within a year, the Mimosa Project began, which diverted the team's resources away from some of

[3] Taken from On-Call Policy .nz ops.

the standard, business as usual matters. They were given additional temporary resources to support the project but this arrangement ended once the project was complete.

Underpinning these changes was the organisational restructure which never took into account that the team was already under resourced by 1 FTE.

It was not immediately obvious until the team started working in the new IRS platform just how significant the impact of the work would be for the team. Furthermore, a number of the team members came on board a year or less before the Mimosa Project ended, at a time when a number of the usual operational processes they would do on the registry were halted for the duration of the project. Once the project was complete and the new registry was implemented, normal operational processes began again.

At the end of the Mimosa Project, there was still a large amount of technical work to be completed, e.g. refreshing some of the DNS systems, refreshing the DNSSEC "signing" systems, and in some cases rebuilding those systems.

In considering whether the .nz Operations Team was under resourced, we reviewed the InternetNZ September 2022 engagement survey. This survey captured the entire organisation, therefore we were not able to identify if the overall engagement results is a true reflection on how .nz Operations Team were feeling. However, the survey reported that staff were feeling fatigued and under resourced, and that there were concerns regarding staff leaving, taking their institutional knowledge with them. These results are not surprising given the changes that have taken place over the last four years, the length of time it took to complete the organisation restructure, and the fact of having three CE's within four years.

The report makes reference to this because in February 2023, InternetNZ met with the CIRA and indicated that having different TTL values on the DS records was not possible and that InternetNZ would need to look into this further. At that point, they had no idea just how much of an impact that would end up having when they did the rollover of the DNSSEC. Unfortunately, the issue was not looked into further because the team had other immediate work pressures at the time and did not have enough resources to complete all the "to do" items as quickly as they would like.

Given the nature of the 24/7 role and the scope of the work changing over the last four years, it would suggest the team have been under resourced.

Ideally, a team who runs a 24/7 "critical systems" on call environment should be large enough to cover staff taking time off in lieu if they have worked longer hours in a day while being on-call, cover for annual and sick leave and provide back up support should an incident require more than one person to manage the incident. While that might be ideal, the reality is budget constraints and the ability to find candidates with the right skill set means it can be an unrealistic expectation for any on-call team to be resourced in such a way.

The team has approval to recruit another full time employee and a fixed term contractor will also be joining the team. This agreement was made before the Incident occurred.

However, it takes time to recruit an appropriate person and a significant amount of time to induct and develop someone into the role (up to six months). This makes for a challenging situation in a 24/7 on call environment.

Having these roles filled will bring the team to 6.5 FTE and will relieve pressure for the team. It is important to review if there is any impact to the work load once the fixed term role ends.

The network

At the time of the second Incident, .nz Operations Team was able to access expert advice from someone who previously worked for InternetNZ. This level of DNS expertise is extremely limited globally and gaining such valuable access, highlights the need to draw on international networks. It also highlights the need for building networks with others in similar time zones or where there is a cross over of business hours to New Zealand such as Australia or Asia. This would then allow .nz Operations Team to connect with someone who they know will be at work and may be able to offer advice. Having networks covering a wider range of time zones ensures staff, particularly when on-call have the ability to connect with others for advice or support regardless of the time or day an incident arises. This is particularly important when taking into consideration how small a team .nz Operations Team, the difficulties of recruiting staff with the right skill set and the time it takes to develop a new staff member in to the role.

What was the CIRA role in the Incident?

It is important to note that the Incident related to the DNSSEC key signing infrastructure within DNS, which is a different system from the DNS registry platform (the "IRS"). Therefore, the CIRA had no responsibility for managing any incident relating to DNS. Instead, their role was to ensure that the IRS would meet the needs of InternetNZ, that there was a seamless migration of the old data into the new IRS, and that InternetNZ was provided training and support. Once IRS became live, it was effectively an InternetNZ responsibility, with the knowledge CIRA were there for support when needed.

The .nz Operations Team, did not contact the CIRA at the time of the Incident due to the time zone differences as it was still Sunday night in Canada and the Incident was not related to the IRS.

The CIRA became aware there was an Incident on 30 May 2023 when Internet NZ asked if they had a DNS architect that might be able to provide support to unpack what the issue was. At that point in time, the CIRA believed that there had been an Incident but the matter had been resolved. It was not until the following day, when the CIRA received further communications from InternetNZ clarifying how critical the Incident was that they immediately arranged a DNS architect to work with InternetNZ.

The support provided by the CIRA was received positively from staff at InternetNZ, comments were made that they went *"above and beyond*". The CIRA confirmed that they are always open to being contacted for advice/support at any time, regardless whether it relates to IRS or DNS.

Opportunities Missed

Missing safety interlocks

From a systems safety perspective the most obvious missing piece in the InternetNZ .nz DNSSEC "signing" environment is any "safety interlock" between the *configured* OpenDNSSEC "DS TTL" time, and the actual *published to the DNS zone* "DS TTL" values.

It should be *technically impossible* for the two to be out of sync, and yet in between the 2014-2018 period and the 2022-2023 period the configured OpenDNSSEC "DS TTL" value has not matched the actual published DNS "DS TTL" value for over 4.5 years. It is basically just a lucky coincidence that this mismatch did not cause an incident earlier (in the 2014-2018 period the OpenDNSSEC configured value was larger than the published DS value, which had the effect of making the DNSSEC KSK rollovers safer rather than more risky).

The OpenDNSSEC "DNSSEC signer" software used has an unfortunate, brittle, design, of taking a *configuration value* that informs it of what it *should assume* another related system – the published DNS information – contains. That design creates the very risk that caused this Incident, that the *configuration value* might be incorrect, or might not be updated when circumstances change.

It is somewhat understandable that the OpenDNSSEC "DNSSEC signer" software chose this design, because it was designed to operate as an "offline signer", with no ability to query the public DNS. But this design choice creates the need to build a safety barrier around the OpenDNSSEC installation, which InternetNZ's .nz Operations Team had not built.

Specifically it should be *technically impossible* to start a "DNSSEC KSK rollover" process if the "DS TTL" configured value in the OpenDNSSEC configuration does not *exactly* match the "DS TTL" value being published in the DNS. The tooling around the OpenDNSSEC programs should simply refuse to start the DNSSEC KSK rollover process, with a fatal error message, if the configuration is wrong in a way that *could* cause an incident like the one experienced on 29-30 May 2023. Or at minimum the inconsistent configuration should be *automatically* regularly and loudly reported to be incorrect, even when a DNSSEC KSK rollover process is not under way.

In systems safety speak, this should be an "Engineering Control" *not* merely an "Administrative Control" (see, eg, 5 Hazard Control Measures summary of control types) – "Engineering Controls" isolate people from the hazard, whereas "Administrative Controls" just ask people to "work more carefully". The "DS TTL" value inconsistency is a sufficiently hidden risk that an Administrative Control is insufficient, and 4.5 years of inconsistency has proven it be inconsistent.

If possible it would also be beneficial to ensure that:

- the IRS registry system "TTL" value (or "DS TTL" value if the CIRA "FURY" DNS registry platform adds a feature for that to be distinct); and
- the DNSSEC signing "DS TTL" configured value

are configured from the same single source of truth.

But even if that is done, the technical "safety interlock" which prevents a "DNSSEC KSK rollover" from *even being started* with inconsistent values should be implemented to avoid situations where

the configuration update has been pushed out to one system but overlooked being pushed out to another system.

Replacing the DNSSEC "signer" servers earlier

Even before the deployment of the new IRS registry platform, the InternetNZ .nz Operations Team have known that the DNSSEC "signer" infrastructure needed to be replaced with newer infrastructure (newer hardware, newer operating system, newer OpenDNSSEC / other signing software install).

If this replacement of the DNSSEC "signer" infrastructure had happened either (a) in parallel with the deployment of the new IRS DNS registry platform (with a different, but similar, "go live" date), or (b) immediately after the production rollout of the new IRS DNS Registry platform, then:

- the discussions of the "TTL" values settings in the new published zones would have been more front of mind; and
- it is extremely likely that a new deployment would have involved a detailed "hand review" of the configuration of the DNSSEC signer software (if only to verify that the desired configuration had been correctly applied when setting up the new servers)

The proximity between the IRS platform "go live" and the "DNSSEC signer" setup would have greatly increased the chance of someone noticing that once again the "DS TTL" values in the DNSSEC signer configuration no longer matched the DNS "DS TTL" value, and that configuration updates were required.

Instead unfortunately the small InternetNZ .nz Operations Team had a crunch period of the IRS go live process, a much needed holiday period, and then were drawn away to other urgent tasks (such as migrating hardware out of a data centre much earlier than planned at the data centre supplier's request). This left an extended gap where the "we need to think more about DS TTL values" general knowledge could be overlooked. (And unfortunately key outcomes like that from the "Mimosa Project" replacing the DNS registry platform did not turn into, eg, calendar events like "2023-05-01 – update DS TTL value in OpenDNSSEC signer to match DNS"; so any updates relied on individual staff memories.)

New registry "parallel run" tests comparing zones without TTLs present

The tool chosen for comparing the output of the old (SRS) DNS registry platform and "DNS zone build" process, and the new (IRS) registry platform "DNS zone build" process unfortunately compared the records *ignoring* the TTL values. (We assume this was for operational convenience, especially if it was querying caching DNS servers to get the zone information and thus could get "lower than configured" TTL values as some time had passed from when the records were first fetched.)

While the “DNS zone output” compare tool did result in identical before/after results for the *content* of the DNS records from the old (SRS) and new (IRS) registry platforms, leading to a successful “go live” of the new IRS registry platform, it did lead to overlooking two TTL related issues:

- For the first week of production with the new IRS registry platform the TTL values in the DNS were 7 days (604800) seconds rather than the intended 1 day (86400 seconds); fortunately we do not know of any incidents caused by this mismatch
- The difference between the TTLs in the SRS generated DNS zones and the IRS generated DNS zones was not noticed. (The SRS generated zones had “DS” and “DNSKEY” records with a TTL of 1 hour / 3600 seconds, and most other records having a 1 day / 86400 second TTL; the IRS generated zones had all records having a 1 day / 86400 second TTL, including the “DS” records, and only the “DNSKEY” and “NSEC3” records having a 1 hour / 3600 second TTL.)

The InternetNZ .nz Operations Team were generally aware before the IRS “go live” that the “DS” TTL values generated by the new IRS registry were defaulting to the same value as the other records. But because their comparison tool did not push it in their face on every compare run it was easier to overlook the difference as “something to look at later” in the rush to get the IRS DNS registry platform into production on time.

Two staff members working together on critical operations tasks

The “DNSSEC KSK rollover” process is the most critical “routine” maintenance task, with the highest risk of problems occurring due to subtle task details, and the highest potential impact if a problem does occur. It is also the most infrequently carried out “routine maintenance” task – by operational policy only being carried out once a year. “Once a year” tasks are barely carried out frequently enough for anyone to remember the process from year to year, even if the same person is carrying out the task – so staff are particularly reliant on written standard operating procedures to carry out the task.

In most safety conscious industries a task with significant risks is always carried out with at least two staff members actively involved, particularly a task that is sufficiently infrequently carried out that no one has the opportunity to learn how to do it solely through repetition. It is also common in many industries that any particularly complicated task is carried out with at least two staff members actively involved.

The commercial aviation industry has probably gone the furthest in codifying the roles of multiple staff members doing critical tasks in a high pressure situation. Commercial airline piloting tasks are split into at least two roles:

- a “pilot flying” whose responsibility is to carry out the flying actions; and
- a “pilot monitoring” whose responsibility is both to carry out additional tasks that would be a distraction to the pilot flying (eg, radio communications with air traffic control to get directions) *and* to monitor the situation and speak up if there is something which needs attention that the “pilot flying” appears not to have noticed

The mere fact of having *two* staff members involved in a critical task, rather than one, necessarily causes more of the process to be vocalised (in spoken or instant messaging text) than would happen if one staff member was doing the task by themself and just mentally tracking the task progress.

Having two staff members involved, especially if one the staff members involved is the one for responsible for "ticking off" items on a standard operating procedure checklist as the other staff member does them, necessarily leads to more detailed monitoring of the task progress.

The InternetNZ .nz Operations Team's choice to allow a single experienced staff member to do the task by themselves meant that this "discussion of the task progress" opportunity was missed.

There are signs in the console logs provided by InternetNZ of, eg, a lookup of the "DS" records for "ac.nz" which do show the 86400 TTL value in among the (voluminous) output, but the significance of this was overlooked at the time the work was being done.

The "two staff members working on the task" approach can be beneficial, as "peer programming" teams have found, even if the two staff members have different levels of experience. For instance:

- if the more experienced staff member is doing the work and the more inexperienced staff member is observing, it is both more likely the experienced staff member will "explain the process" as they go (vocalising things that would otherwise go unspoken) and it is also more likely that the inexperience staff member will ask more questions that might prompt investigation. Even a question like "why does that output say 86400 when the standard operating procedure says we can proceed after an hour" may have lead to a discussion which avoided this Incident unfolding to the extent that it did (eg, the other .nz second level domain KSK rollovers may not have been started until a suitable explanation for the discrepancy had bene found)
- if the less experienced staff member is doing the work, mentored by a more experience staff member, then the less experienced staff member is more likely to check they are doing it correctly by asking questions *and* the more experience staff member will be primed to *expect* there to be mistakes made by the less experienced staff member and expecting to steer the process in a safe direction.

The process of having two staff members involved in a critical task does not guarantee that all issues will be caught. Among other things both staff members are prone to confirmation bias (finding evidence to confirm what they believe is true is actually true). But many industries have found it has helped. And in addition if an incident does occur, you start the Incident response with at least two staff members with detailed knowledge of the steps taken to reach the Incident state.

True "canary" DNSSEC KSK rollover test

Many IT operations tasks have sufficient external dependencies that it is impossible to tell – for certain – that the task will be successful *in production* without doing the task in the production environment. (Test and staging environments can only reproduce some, but not all, of the production environment, and the portion that they reproduce is not necessarily the portion necessary to identify an issue.)

Software development and deployment processes have developed the concept of a canary deployment where a specific change will be deployed into production in a limited manner. For instance, it might only apply to a limited subset of uses of a feature, or a limited subset of users.

Several technical people we spoke to during this review assumed that the earlier "ac.nz" DNSSEC KSK Rollover was intended to be a "canary" deployment – testing the DNSSEC KSK Rollover separate from the other .nz second level domain KSK rollovers. And legitimately asked the question why, after that "canary deployment" had been reported to have problems – on the afternoon of Monday 2023-05-29 – that the InternetNZ .nz Operations Team had "carried on" with the other second level domain KSK rollovers.

It is a reasonable question, but as described in the timeline and technical Incident findings the "ac.nz" DNSSEC KSK rollover was *not* a true "canary" test deployment. Instead the "ac.nz" DNSSEC KSK rollover was done first, by hand, to validate that the *new tooling* to integrate with the new IRS registry platform (and add/remove "DS" and "DNSKEY" records) had operated correctly. Once that tooling had been proven to work in production, the rest of the task was carried out *without waiting long enough* to gather reports of issues as one would have done in true "canary deployment" testing.

Specifically for the first ("ac.nz") DNSSEC KSK rollover to have been a *true* "canary" test it would have been necessary to wait a lot longer – ideally at least until the next calendar day – for any reports of issues to arrive. Before *starting* the other parts of the DNSSEC KSK rollover for the other .nz second level domains.

If there had been a full day between the "ac.nz" DNSSEC KSK rollover and the other .nz second level domain DNSSEC KSK rollovers being started, the reports of problems resolving "ac.nz" domains would have arrived before any other work started. Instead all the other .nz DNSSEC KSK rollovers were already *well under way* by the time the first report arrived – the accident was already in progress – and the only remaining chance was to "recover from the accident in progress".

In addition if the first "canary" test ("ac.nz") had been found not to go ideally, and a plausible "root cause" had been identified, it would have been possible to do *another "canary" test* with a single other .nz second level domain (ideally another small one) and verify that the *altered process* did properly avoid the Incident. If, as here, the true root cause was not immediately identified and the second "canary" test also ran into issues, at least the "blast radius" of the second phase of the Incident would be much smaller, have affected fewer users, and by then the "steps third parties can take to mitigate the issue" would be much better understood.

Disabling "ods-enforcer" cron job on Monday 2023-05-29

With hindsight, the most obvious "pause the accident in progress" step that could have been taken to avoid the second half of the DNSSEC KSK rollover Incident would have been to disable the 22:45 daily "cron" job that ran the "ods-enforcer" process. It was that process which (a) noticed "more than the *configured* DS TTL time has passed" and (b) updated the OpenDNSSEC database state to record that the "ods-signer" (DNSSEC signing) process no longer needed to use the old KSK key for signing the ZSK records.

If running the "ods-enforcer" process had been delayed even 24 hours, the majority of the Incident would have been avoided as – by coincidence of that action – enough time would have passed that the next step that "ods-enforcer" wanted to take would then have been safe.

While it is very likely that disabling the "ods-enforcer" cron job on the night of Monday 2023-05-29 would have *avoided the Incident in 2023,* it is also likely that that avoiding the majority of the Incident could have led to the "ac.nz" DNSSEC KSK rollover Incident being attributed to "a one off glitch", or remaining attributed to the original conclusion (removing the "DS" / "DNSKEY" records too soon). Which would have resulted in the *true* cause not being identified in 2023, and a similar incident occurring during the next "annual maintenance procedure" in 2024. As painful as the Incident was in 29-30 May 2023, at least it was sufficiently significant to prompt both an internal and external review, and identify the true contributing factors so that they can be addressed.

Importantly, however, is that on the night of Monday 2023-05-29, the InternetNZ .nz Operations Team:

- did not have as detailed an understanding of how the OpenDNSSEC "signer" software worked as they needed to be certain that the "ods-enforcer" cron job could be safely disabled in the state they were in (it was a very old installation, by previous staff, and something of a "black box")
- did not have access, in the 6 hours available to make the decision, to external support that could tell them for certain whether or not they could disable the "ods-enforcer" cron job safely (of note it was evening/night in North America at the time, where many DNS experts are based, including those working for CIRA their DNS registry platform partner)
- knew that it was critically important that the OpenDNSSEC software continued to perform DNSSEC signing functions normally otherwise there would be a larger problem (once DNSSEC signatures start expiring they are also considered "bogus", producing the same symptoms as experienced in this incident)
- were, from knowledge of other DNSSEC incidents world wide, extremely wary of taking actions that might make the situation worse; DNSSEC is sufficiently fragile that it is easy to turn a "bad" situation into a huge disaster by doing the wrong thing at the wrong time attempting to "fix the problem"
- by the time the InternetNZ .nz Operations Team even knew there was an incident it was fairly late in their normal work day, reducing their ability to concentrate on independently researching whether "ods-enforcer" could be safely disabled in parallel with all the other incident review they were doing; and there was no fresh "second shift" to hand that task over to

We conclude that "disabling the ods-enforcer cron job" was, at best, with the information available on Monday 2023-05-29 evening, a "line ball" call. It is obvious with hindsight that a different call being made on that "line ball" would have made a difference; but we do not believe it was reasonable to expect it to be known, let alone obvious, at the time the InternetNZ .nz Operations Team had to make that call.

The true conclusion here is that it is important that the InternetNZ .nz Operations Team have a deeper team-wide understanding of the detailed functioning of the tools with which they are working. So that they can have a more detailed mental model of what can be safely changed about the tool's operation in the event that something is not going according to expectations. (As it happens OpenDNSSEC does have a very detailed DNSSEC key rollover safety analysis written by

the authors of the software; but that analysis is not something you can read in the pressure of incident response and confidently make a decision based on what you read.)

Doing the KSK rollover first on the standby DNSSEC signing chain

InternetNZ's DNSSEC signing infrastructure has two independent "DNSSEC signer" servers, in separate data centres, which both run in parallel. The "active" DNSSEC "signer" is the one that is being published to the public DNS, and the "standby" DNSSEC "signer" is the one that is not published. But otherwise both the "active" and "standby" DNSSEC signers are expected to be functioning correctly and consistently at all times.

InternetNZ .nz Operations Team's standard operating procedure was to do the "KSK Rollover" on which ever DNSSEC signer had least recently had the "KSK Rollover" procedure performed, irrespective of whether it was the active DNSSEC signer or the standby DNSSEC signer. In May 2023 this worked out to be the active DNSEC signer first, due to when the active and standby signers were last swapped over. The choice (in May 2023) to do the DNSSEC "KSK Rollover" on the active signer first has advantages and disadvantages.

Doing the "DNSSEC KSK Rollover" on the active signer first:

- simplifies confirming that the KSK rollover has gone correctly (the result are immediately publicly visible)
- ensures that the standby DNSSEC signer is in full functioning state (the old configuration) throughout the KSK rollover of the active DNSSEC signer
- but, on the down side, as in this Incident, if anything goes wrong, the results are immediately publicly visible and may impact third parties

Doing the "DNSSEC KSK rollover" on the standby signer first:

- complicates the process of validating that the DNSSEC KSK rollover has occurred correctly
- but that validation can be done, and the process corrected, without the results being publicly visible, and thus the chances of third parties seeing a broken state is much lower
- however it does also risk "breaking the standby DNSSEC chain" (by starting a KSK rollover that does not go cleanly) at the same time as something else happens to the primary DNSSEC signer (eg, a data centre incident), so there would be no redundancy left

It is an operational decision which of these choices of tradeoffs is best.

Some extremely critical functions avoid some of the disadvantage of "working on the only standby/backup" by having *more than* N+1 redundancy: for instance with N+2 redundancy you might have three systems – the active one, the "always ready to go" standby one, and the "in maintenance" one. Having an *additional spare* enables doing the maintenance steps, while still having "N+1" redundancy on the critical feature. For DNSSEC key signing in particular there are some additional tradeoffs for attempting to have "N+2" redundancy, especially relating to the size of DNS answer records; but these could possibly be mitigated by only including the "in maintenance" DNSSEC signer in the public records when it was "about to be used", and rotating

the roles among the DNSSEC signers, so each was used as active / maintenance / standby-ready in turn.

We do not have a clear conclusion on whether this "first DNSSEC KSK rollover after a new registry platform was deployed" should have been done first on the "standby signer" or not, but we do recommend the InternetNZ .nz Operations Team consider whether doing the DNSSEC KSK rollover "in public" (first) is the best approach for future DNSSEC KSK rollovers.

Switching to publishing the standby signing chain

As described above, InternetNZ does have a second DNSSEC signer, with an entirely independent signing chain (its own KSK and ZSK), which is expected to always be "ready for action" – including the "DS" and "DNSKEY" records for both the active and standby DNSSEC trust chains present in the DNS zones generated by both the active and standby "signers" (so they are "pre-published").

With the benefit of hindsight, it appears the InternetNZ .nz Operations Team could have chosen to switch to publishing the standby signing chain – which should have been seen as validly signed by all validating recursive DNS servers, based on cached DNS records (*including* the old cached "DS" records, which did include the "KSK" record of the standby signer at each level).

However:

- switching from one DNSSEC signing chain to another is a bit like leaping from the top of one tree to the top of another tree: if you make the jump you really hope it is going to support you as you land
- the InternetNZ's .nz Operations Team process for switching to publishing the standby DNSSEC signer was only semi-automated (multiple steps to initiate manually)
- every other time the InternetNZ .nz Operations Team has switched which DNSSEC signer was published they had done a large volume of manual checks to confirm everything was in the right state to make the transition
- on the evening of Monday 2023-05-29, and the early hours of Tuesday 2023-05-30, the InternetNZ .nz Operations Team did not have sufficient confidence in their understanding of the true root cause of the Incident to (a) be certain that the standby DNSSEC signing chain would not also be affected, (b) that they could safely transition from the existing active DNSSEC signing chain to the standby DNSSEC signing chain in a useful time frame, and (c) that the transition would not also be affected by caching DNS server state held in third party servers

So while that switch, with the benefit of hindsight, seems an option that was likely to be successful if carried out correctly, it is entirely understandable that it was not considered a realistic option on the evening of Monday 2023-05-29 and the night of Tuesday 2023-05-30. Particularly given the strong desire not to make any "sudden moves" that might make the problem worse – suddenly switching DNSSEC signing chains is the type of "recovery mechanism" which has, in other DNSSEC incidents, turned a bad situation into a worse situation.

For "switching to the other DNSEC signing chain" to be a realistic recovery step, it would need to be:

- much more automated; and
- have very strongly automated “sanity checks” that all possible combinations of records that might be cached would still be consistent after the switch; and
- a more detailed, advanced, analysis of when “switch to the other DNSSEC signing chain” is a safe recovery option to evaluate

Such significant decisions cannot be safely made in an “incident response” context, other than “that feels risky, let’s not try that”.

Reactivating the old “active signer” KSK temporarily

At the time that the effects of the DNSSEC KSK rollover Incident were first felt, InternetNZ did still have the key material (in their HSMs) for the old KSK values. With the benefit of hindsight it would have been possible to reintroduce those keys into the OpenDNSSEC environment, and start using them again as active “KSK” keys *in parallel with the new “KSK” keys*. This could have been used to build a temporary bridge between the cache “DS” records and the published “DNSKEY” records. And in theory the affected validating caching recursive DNS servers would have recovered as soon as they fetched the updated “DNSKEY” record and its signatures – within an hour – restoring the trust chain that they expected. Then the old KSK keys could have been removed again, safely, a day later, once *all* validating caching recursive DNS servers had found the new “DS” records.

While theoretically possible, and even allowed for in the OpenDNSSEC key state transition diagrams to move between the “unretentive” state (fewer and fewer caching servers know about the key) and the “rumoured” state (more and more caching servers know the key), it was not a reasonable option to consider during the Incident because:

- the InternetNZ .nz Operations Team had never reintroduced a KSK key after removing it, and had no written process for doing it
- it is a very delicate process, and under incident response pressure is not the time to be inventing a new critical process sequence; and
- even though it is noted by OpenDNSSEC as a possible state transition, there does not appear to be a documented sequence for *temporarily* reintroducing a KSK key that was previously used (so best case it would be introduced as the “new new” KSK, creating a new problem later to remove that “new new” key and get back to just the intended “new” key)

So as hopeful as “just hit undo” looks from the outside, there was no easy “undo” option available to the InternetNZ .nz Operations Team during the Incident response.

Once the Incident had occurred their chosen path – encourage third party recursive DNS server operators to mitigate the effects of the Incident for them – was the lowest risk next step, avoided risking causing more problems, and was certain to result in a resolution to the Incident within a fixed period of time (around 12 hours from when the InternetNZ .nz Operations Team finally understood the true root cause).

Report recommendations for future improvement

These recommendations are ordered with the more important recommendations first, and then loosely grouped by related topic. The recommendations beginning "consider" raise additional topics which we believe that InternetNZ should investigate further, without making a firm recommendation that they should be done; all of those items have operational tradeoffs that need additional consideration beyond the scope of this review.

High impact risk infrequent maintenance should be notified in advance

Infrequently done maintenance tasks, especially ones which carry a risk of a high impact on third parties and may require third parties to take impact mitigation action, should be scheduled and notified in advance. For instance the InternetNZ "status" for the planned work could be created to notify when the work is going to take place (eg, which day), and that status page link distributed to relevant Aotearoa | New Zealand DNS registrars and recursive server operators in advance.

In addition to assisting third parties with correlating symptoms observed with known changes taking place, which speeds up identifying possible causes and possible mitigations for the symptoms, advanced notification also greatly increases the chances of the InternetNZ .nz Operations Team receiving timely notifications that adverse symptoms are being observed. (Rather than, as in the 29-30 May 2023, those reports arriving two hours after the change.)

High impact risk tasks should be done by multiple people together

Tasks which carry a risk of a high impact on third parties benefit considerably from having the attention of more than one person focused on the task in real time. Having multiple pairs of eyes on the task progress increases the chances of noticing "something unexpected" in the task standard operating procedure, and investigating it before the task is completed to an "accident in progress" state. The extra staff resources available for the task also greatly increases the chances of more detailed cross checking being done, as the staff members confirm each others assessment of the progress to date, and whether it is successful.

Handle unexpected symptoms during maintenance as "an incident"

If unexpected symptoms arise during a high impact risk maintenance event, then those unexpected symptoms should be treated as "an incident" in their own right. Formally documenting and investigating even "near misses" brings a lot of insight into what could possibly go wrong, and what the possible consequences could be if the Incident had continued further. And helps with identifying future precautions that could be taken to avoid a reoccurrence of those unexpected symptoms in future work, helping mitigate potential risks without requiring major disruption. The commercial airline industry, in particular, has seen significant safety and reliability improvements from unconditionally investigating even "near misses".

In addition practicing the "operational incident management" process even in the context of an "unexpected symptoms" incident means all staff are familiar with the process, and ready to use that process when it is needed for a more serious incident. These "unexpected symptoms" should at minimum be reported up the management chain to InternetNZ "General Manager" level, so there is senior management overview of "near misses" and what resourcing is needed to mitigate the risks encountered.

Formalise communication channels to recursive DNS server operators

The InternetNZ .nz Operations Team has good established formal channels for communicating with their registrar partners (who facilitate domain registration for end user registrants), particularly around registry platform notifications.

There should also be a dedicated *seldom used,* for critical recursive DNS server operations notifications only, notification channel for recursive DNS server operators (at ISPs, major corporates, etc), which can be used to send timely alerts of issues like this. In a "situation normal" year, that notification channel should only be used to send a yearly "the next annual DNSSEC KSK Rollover will be next week" notification.

Any such *operational notification* channel **must only** be used to send operationally relevant notifications, that require immediate attention. If the notification channel is "spammed" with irrelevant messages, people will unsubscribe, or stop reading the messages, and the "timely notification of issue requiring urgent attention" purpose will be defeated.

(The InternetNZ .nz Operations Team did a good job of utilising notification channels they already personally had, including ones associated with the NZNOG group, which reached many relevant DNS server operators at ISPs. But other recursive DNS server operators, eg at large corporates, probably only found out later, via the news.)

Ensure OpenDNSSEC "DS" configuration to matches DNS reality

The *configured* OpenDNSSEC "assuming this is the DS TTL" values need to be updated to match the current values in the published DNS "DS" TTL values – ie set back to the 1 day (86400 seconds).

If it becomes possible to configure a new "DS" TTL value in the new IRS registry software (distinct from the other records), then this new "DS" TTL value needs to be reflected in the configured OpenDNSSEC DS "TTL" value. Otherwise the OpenDNSSEC "ods-enforcer" daemon is making assumptions about the safe times to proceed to the next stage of rollovers based on misleading information.

In particular there needs to be clear documentation that if the "DS" TTL is changed in the DNS then it *must* be changed in the OpenDNSSEC "DS" TTL configuration at the same time.

Configure OpenDNSSEC and DNS "DS" timers from a single source

To help ensure that the OpenDNSSEC configuration for "ods-enforcer" of the "DS TTL" matches the DNS registry configuration of the "DS" TTL, the two should be configured from a single source (ie, so it is only hand configured in one place).

This single source could be:

- the IRS registry platform (with the OpenDNSSEC configuration value extracted from the IRS registry platform, or the published DNS)
- a central configuration management system (eg, Ansible) that configures both the IRS "TTL" values via an API, and the OpenDNSSEC "ods-enforcer" configuration, based on a single configuration file of "chosen registry parameters".

(There is still a risk that the two could be out of sync if an update is pushed out to one system but not the other, but having a single configuration source – "Don't Repeat Yourself" – reduces the window within the two can be out of sync.)

Add guard rails around OpenDNSSEC commands

The raw OpenDNSSEC commands are built in a brittle way, relying solely on configured values to inform it of values configured elsewhere, to enable entirely offline usage. In addition in the InternetNZ .nz Operations Team usage there are multiple configured profiles (different for the .nz top level domain, and for second level domains) and the correct profile has to be used for the correct task.

To mitigate the risk of the OpenDNSSEC configuration not matching reality, or the wrong configuration profile being used for a task in future, implement wrapper scripts around the OpenDNSSEC tools which:

- ensure that the OpenDNSSEC configuration values that need to reflect external systems (such as the "DS" TTL) to reflect the *published in the DNS parent zone* "DS" values, and refuse to proceed if they do not match; and
- auto-identify which OpenDNSSEC policy section applies to a given domain, instead of relying on this being user supplied as an additional parameters. (This was not a cause in this Incident, but could be a cause of a future incident.)

In addition the "ds-seen" step in the OpenDNSSEC KSK rollover process should be automated based on an *automatic* tool based look up of the published DNS, rather than solely reliant on a human check of the "DS" records. (This was not a cause in this Incident, but could be a cause of a future incident.)

Document change of "DS" TTLs in .nz zones since November 2022

The change to the new IRS registry platform effectively resulted in the rollback of a 2014 InternetNZ .nz Operations Team policy that "DS" records *for end user registrations* would be 1h (3600 seconds) to permit faster recovery of end user DNSSEC rollover issues.

This "faster recover" for end users is no longer available at this time, and end users need to plan their DNSSEC operations around the fact that "DS" changes published into the .nz registry zones will not necessarily have been retrieved by all validating caching recursive DNS servers until 24 hours has passed.

This means that *end user* authoritative DNS server operators need to be advised to update their own DNSSEC signing, and especially key rollover, practices to take this longer period into account.

Consider reducing "DS" TTLs back to 1h for faster recovery

Investigate whether the .nz registry published zones can have the TTL (time to live) values for the "DS" records changed back to 1 hour (3600 seconds) to match the previous decade of .nz policy. This may require a feature change to the CIRA "FURY" registry platform used by InternetNZ, but such a feature request should be prioritised by InternetNZ.

Internet Best Practice is converging on 1 hour (or shorter) "DS" TTL values to enable faster recovery, as InternetNZ had set from 2014-2022 (see, eg lightning talk on DS TTLs at DNS OARC

40). And even shorter “DS” TTL times are being investigated by other large DNS server operators with relatively minimal workload impacts on DNS servers.

Consider aligning the “DS” / “DNSKEY” TTLs to simplify timing analysis

The published .nz DNS zones currently have a “DS” value of 1 day (86400 seconds) and a “DNSKEY” value of 1 hour (3600 seconds), we believe due to the TTL of the “DS” records being based on the IRS registry DNS export whereas the TTL on the “DNSKEY” records is based on the OpenDNSEC “ods-signer” configuration. This means new “DNSKEY” records are certain to have been fetched everywhere after 1 hour, but new “DS” records may not have been fetched for up to 1 day. The widely varied timings make analysing the “safe time” to take DNSSEC KSK rollover steps more complicated for humans to analyse, as they must remember which timer is relevant at which step. (Automated tools, fortunately, usually have this dependency analysis properly automated.)

Aligning the values of the “DS” and “DNSKEY” TTLs at, for example, 1 hour, as was the case from 2014-2022 simplifies this analysis. And also leads to a caching recursive DNS server being more likely to fetch both the “DS” and “DNSKEY” records on the same cadence, increasing the chances it will have fetched matching records. (Versus the current configuration where it may rely on a 23+ hour old “DS” record, while attempting to use the new “DNSKEY” record, creating a complicated timeline to reason about.)

Document how to safely "pause" a DNSSEC key rollover

The InternetNZ .nz Operations Team should create a standard operating procedure for pausing an in-progress DNSSEC key rollover, at the next available safe point. This would ensure that if “unexpected symptoms” are observed, there is a clearly understood path to get to a safe place to stop indefinitely while it is analysed further. In the ideal world, these “pause points” could be stopped at for sufficiently long that an “accident in progress” due to rushing steps could be entirely avoided.

OpenDNSSEC has a well thought out “state transition” diagram for DNSEC KSK rollovers, and in general it is safe to stop at any of the states indefinitely. If the InternetNZ .nz Operations Team had a documented procedure for “pausing” the .nz second level domain KSK rollover, that they knew they could rely on, on the evening of Monday 2023-05-29, it is much more likely they would have chosen to pause that rollover (by disabling the “ods-enforcer” cron job earlier).

Create “worst case caching” recursive DNS server for monitoring rollover progress

One of the biggest investigation hurdles during the 2023-05-29 early investigation of the problem was that the InternetNZ .nz Operations Team did not have a way to reproduce the problem.

During DNSSEC KSK Rollovers we recommend that InternetNZ *deliberately create* the worst case “cached data” in a dedicated validating recursive DNS server, by *immediately before* the rollover stages are published to the public DNS, (a) flushing the DNS server cache of that server, and (b) using that validating recursive DNS server to look up the older records. This ensures it caches the old records at the “last possible moment”, and thus will retain them as long as any other caching recursive DNS server on the Internet. And then continuing to investigate DNS lookup issues

through that deliberately created “caching old data” server, to monitor progress of the DNSSEC KSK rollover steps.

Validate production change process with a true “canary” rollover

Infrequently performed tasks, particularly those that are difficult to determine are fully tested in a non-production environment, should have a “canary” test performed, with ample time allowed to notice any issues arising before *starting* the rest of the task.

More specifically, the “canary test” should be performed:

- on an entirely different day from the “main” rollover tasks (allowing at least 24 hours to notice symptoms, ideally longer)
- without *starting* the other parts of the task, so that if unexpected symptoms are encountered it is certain that only the “canary” is affected.

Ideally the “canary test” would be done with the *least production critical* data possible. For instance *both* a “low number of registrations” DNS zone *and* one with few users relying on it.

Consider creating a *specific canary test* domain, managed via the same OpenDNSSEC process as the other .nz second level domains, but with only test registrations in it. And ensuring that is (a) published to the public DNS, and (b) monitored externally for DNSSEC rollover issues. Such a true “canary test” would, likely, have found this configuration oversight before the main .nz second level domains DNSSEC KSK rollovers had *started*, and reminded the InternetNZ .nz Operations Team there was an important configuration update overlooked.

Automate safety checks around DNSSEC KSK rollovers

The current InternetNZ .nz Operations Team standard operating procedure for DNSSEC KSK rollovers relies on several manual checks that the process is proceeding as expected. These checks should be automated, and ideally regularly done via a monitoring system which can surface the current state of the DNSSEC KSK rollover into a dashboard (good, or bad).

Automating these checks both increases the visibility of the current state of the DNSSEC KSK Rollovers (avoiding the need to reverse engineer that state from multiple sources), and also ensures all the checks are done frequently during the process.

Combined with the “worst case caching” validating recursive DNS server above, these automated checks can also compare the results of mixing old cached records and newly fetched records together. Any *safe* DNSSEC KSK rollover must be done in an order, and speed, that *any* cached record can be mixed with *any* newly fetched record, and still give valid results. Comparisons involving both old and new records are difficult to do by hand, but fairly easy to automate.

Automate the “manual safety checks” before publishing standby zones

One of the reasons given by the InternetNZ .nz Operations Team for not considering swapping to the “standby” DNSSEC signed zones, was that their standard operating procedure for swapping over required a lot of manual checks. These checks can, and should be automated. As with the old/new cached records comparison, there is a need for the automate checks to consider any combination of cached “currently active” signed records and “currently standby” signed records, to

ensure all combinations are valid. That results in a lot of checking required, which is ideal for being delegated to automation.

If the fact that the "standby signer" is not "published" makes this more difficult to automate, then consider at least "internally publishing" the standby signer DNS zones somewhere that the automatic checks can see *both* the standby signer DNS zones *and* the currently active signer DNS zones, and cross validate them against each other automatically.

Further automate swapping between active and standby signers

As described by the InternetNZ .nz Operations Team the process of swapping which is the "active" DNSSEC signer and which is the "standby" DNSSEC signer – ie changing which one is published to the public DNS servers – is a semi-manual process, involving multiple manual checks (addressed above), and multiple semi-automated steps.

Once the "safe to switch" checks are fully automated, and the automated checking is trusted (ie, hand validated over time), the process of swapping which DNSSEC signer zones are published should also be automated. Ideally there should be a single configuration value which determines which signer's zones are published, and a single command to run that orchestrates changing over the published DNSSEC signer.

If swapping between the active and standby DNSSEC signer was (a) fully automated, and (b) known to be a safe robust process, then the InternetNZ .nz Operations Team could have considered this as an option for recovery from their KSK signing process. With it as a "manual checks required, manual steps required" process, it was never a viable recovery step for anything other than a catastrophic business continuity event.

Develop a process to ensure BAU task prerequisites are completed before BAU tasks

One of the biggest operational oversights leading up to this event was that the "Mimosa Project" (to select and deploy the new IRS registry platform) was aware that the "TTL" values generated by the new IRS (CIRA FURY) registry platform were different from what had previously been done. That was discussed as recently as February 2023 when CIRA and InternetNZ met to discuss "BAU operations" of the registry platform after the deployment project was complete.

But the wrap up of the Mimosa Project did not successfully hand over the "must look into impacts of DS TTL record changes" task to the InternetNZ .nz Operations Team "BAU" ("Business As Usual") process in a way that ensured the critical configuration dependency would be addressed in time.

This type of "project wrap up", "tasks left to complete handed over to BAU" needs a more formal process that ensures that (a) any "tasks left to complete" are captured in sufficient detail that what to do is still obvious 5-6 months later, and (b) any tasks that have critical timing dependencies (eg "must do before next KSK rollover") have that dependency requirement formally captured, so that it is obvious to anyone embarking on the dependent task that there is an outstanding dependency.

Review and Update the Business Continuity Plan

Review the BCP and reach an agreement as to:

- what is considered a critical incident (not just when there is a natural disaster)
- how this should be raised eg when is it appropriate to call someone in the middle of the night? When should a “heads up” email be sent to be reviewed next morning?
- develop an incident response plan that relates to operational matters like partial outages due to technical faults.

It is important all staff are aware of the BCP and that it be discussed regularly to ensure it is up to date and fresh in everyone’s mind. This can be done the following ways:

- ensure the BCP is part of every staff of induction programme
- where appropriate, run readiness activities such as desktop exercises with scenarios to help staff to recognise and understand what to do when an incident takes place
- develop case studies/scenarios with examples of prepared comms – using this latest Incident as a case study to document “what to do when.”

Support .nz Operations Team to build and use their international network

Because of how technical and specialised DNS work can be, it is important ***all*** team members have the ability to build their network internationally so they can share and gain knowledge from others within their industry.

The whole team should be encouraged to build these relationships as it is always easier to make contact with someone if you have already met them in person. This is particularly important in a 24/7 on call environment when you have an incident outside the usual business hours and your most available source of assistance may be someone in a different time zone.

InternetNZ should encourage more team members to attend conferences. We recommend letting team members take turns at attending conferences.

Here are some examples of related conferences:

- DNS OARC ("Operations, Analysis, and Research Centre) workshops offer a number of ways for organisations to participate in its activities https://www.dns-oarc.net/oarc/agreements..
- IETF (Internet Engineering Task Force) meetings, particularly the DNSOPs working group sessions (https://www.ietf.org/how/meetings/, https://datatracker.ietf.org/wg/dnsop/about/). IETF meetings are held three times a year, rotating locations around the world.
- ICANN, is primarily about "international arrangements, business and process" functioning of the Internet, including the DNS, but does also include technical sessions.
- NZNOG -- (New Zealand) annual conference, attended mostly of ISP operators (with talks from related people);

- AUSNOG -- (Australia) annual conference, attended mostly of ISP operators (similar to NZNOG, but more of an Australian audience)
- APNIC conference – APNIC is the "Internet Registry" authority for the Asia Pacific region, and has an annual conference in a different member country each year;
- Apricot conference -- annual conference, largely aimed at the same audience as the APNIC conference, but deliberately run at a 6 month offset from the APNIC conference and organised by another committee who felt there should be two conferences; also rotates around the Asia Pacific countries.

For this to happen, the team need to know they have the ability and support to take time away from their business as usual work to focus on developing these important networks.

InternetNZ could also consider a formal relationship with an organisation in Australia, or Asia, where there is an overlapping of timezones, that will allow the .nz Operations Team to escalate problems that occur (or continue) "after business hours" in Aotearoa | New Zealand.

This would allow the .nz Operations Team to have a pre-arranged path to request more assistance from other DNS experts, during those DNS experts daytime, rather than relying solely on "personal favour" requests, or fellow team members who may be in need of sleep/rest.

Review .nz Operations Team resourcing regularly

It is acknowledged an additional 1.5 FTE has been approved prior to the Incident taking place. Ensure there are regular check-ins to see how that extra resource is being used and what the impact of that resourcing will be for the team when the fixed term contractor completes their contract.

Status sites should be hosted to not rely on monitored infrastructure

While it was not specifically reported as an issue during the May 2023 incident, we recommend that the InternetNZ "status" page be hosted in a way that does not rely on InternetNZ run infrastructure to be reachable. In particular the current location, https://status.internetnz.nz, relies on both the nz TLD DNS being resolvable, and InternetNZ's own DNS being resolvable. (The underlying hosting, via CNAME, is at an independent third party.)

Consider registering, eg, status-internetnz.net to be the primary domain referenced for status information without reliance on the .nz TLD DNS resolution, and turning status.internetnz.nz into a CNAME or HTTP(S) redirect to that.

Consider doing KSK Rollover on standby signer first

DNSSEC "KSK Rollover" tasks done on the standby signer have much less risk of immediate production impact. Consider whether the DNSSEC KSK Rollover task can be completed on the standby signer first, including validating that the "would be published" DNSSEC signed zones are valid at all times during that rollover, before doing the DNSSEC KSK Rollover on the active production DNSSEC signer.

Care is still required when doing the DNSEC KSK Rollover on the "standby" DNSSEC signer, even though it is not immediately published, because if the "standby" signer zones get into an unsafe state, then there is no longer a viable "standby" for the active signer (and one is "operating without a safety net" for the business continuity plan). But the increased time to fix (many hours)

and lower immediate impact (none, if not yet published) makes the change to operational process well worth considering.

Consider only doing KSK Rollover on standby signer (then swap)

If (a) the decision is made to do the KSK Rollovers on the standby DNSSEC signer first, and (b) the process of switching which DNSSEC signer is published is fully automated, then another option opens up: *always* do the DNSSEC KSK rollovers on the standby signer. And then when they are complete, make that "just rolled over" signer the active one. After a safe period of time, the previously-active-now-standby DNSSEC signer can then have its DNSSEC KSK rollover, again on the "standby" side.

Consider doing KSK rollovers in two batches, six months apart

If the process is sufficiently tested and automated to only do DNSSEC KSK Rollovers on the standby side, then put the "already rolled over" signer into production, then another useful option to consider would be to stagger the DNSSEC KSK Rollovers to happen in two parts – six months apart – instead of one burst, once a year.

This increases the amount of practice the InternetNZ .nz Operations Team gets with the infrequent "DNSSEC KSK rollover" process, while still ensuring every KSK key is rolled over "once a year" as per InternetNZ's DNSSEC practice statement. These more frequent intervals increase the confidence that the automation for doing DNSSEC signer publication swap overs work correctly, and can be relied on in the event of an incident. Overall there is not much more work required of the InternetNZ .nz Operations Team, it is just split into two parts. Which potentially gives more of the team members recent exposure to the steps required (particularly if two or more members are involved in each rollover, as recommended earlier).

Consider moving ns[1-7].dns.net.nz to names under .nz TLD

The .nz top level domain DNSSEC KSK Rollover, itself, proceeded normally without problems. But there were still impacts on the on validating recursive servers attempting to resolve "NAME.nz" direct registrations into the .nz top level domain. Including at least one case where the "NAME.nz" DNS information does not obviously rely *directly* on anything under an affected .nz second level domain. This occurred despite "dns.net.nz" *itself* not being publicly DNSSEC signed. We believe a combination of the DNS "QNAME minimisation" feature and the fact all the .nz DNS servers are under an affected .nz second level domain, contributed to the impacts of this Incident: ie, there was a step where the validating recursive DNS server attempted to validate the "net.nz" information it was given (eg, nameservers) and encountered bogus results and gave up.

Consider reserving a series of names in the .nz top level domain to use for the public DNS nameservers for the .nz top level domain and .nz second level domains. Either *directly* in the .nz top level domain (eg, ns1-tld.nz) or at least in a second level domain instead of a third level domain (eg, ns1.tld-dns.nz).

Care will be required in planning this transition, and this "once in the registry history" type of maintenance change task should obviously be notified publicly in advance, as recommended earlier. (We would also recommend that the planned cutover process be reviewed by third parties in advance, to benefit from global DNS operational experience in performing such changes.)

Consider building procedure to reinject old KSK into OpenDNSSEC signing

One of the "missed opportunities" described above was that there was a technical option to "reinject" the old KSK key back into the publish DNS for period of time, so that it was used as a KSK signing the (unchanged) ZSK *in parallel with the newly emerging key*. This was not considered as a viable option by the InternetNZ .nz Operations Team as they had no prepared procedure for it, and it is sufficiently complex to do that they did not want to make up a procedure on the fly.

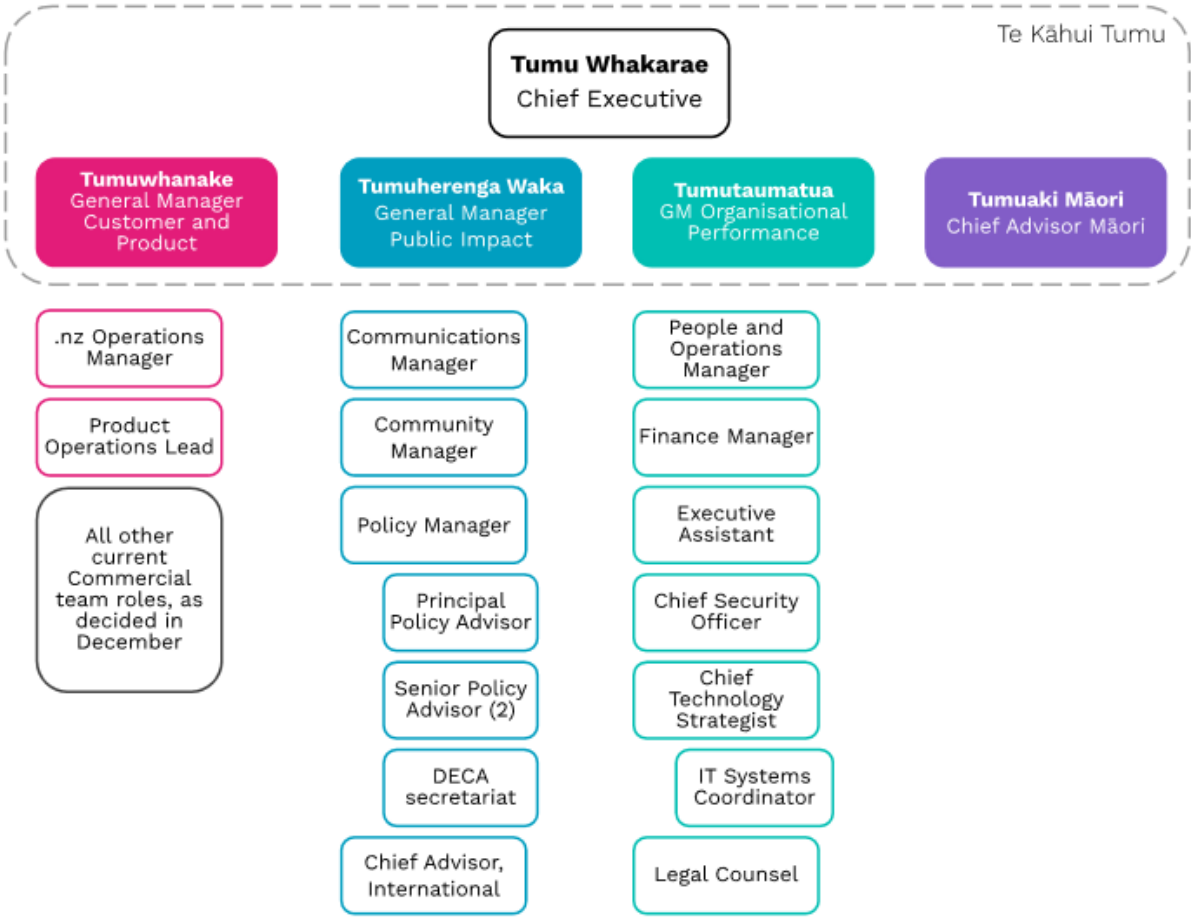
Consider developing and testing a procedure to reintroduce a "just expired" KSK back into the published DNS, including having OpenDNSSEC use it for signing the ZSK, to have available as an emergency recovery procedure. Careful thought will also be required as to how to remove the "reintroduced, recently expired" KSK from the published DNS again after it is no longer wanted.

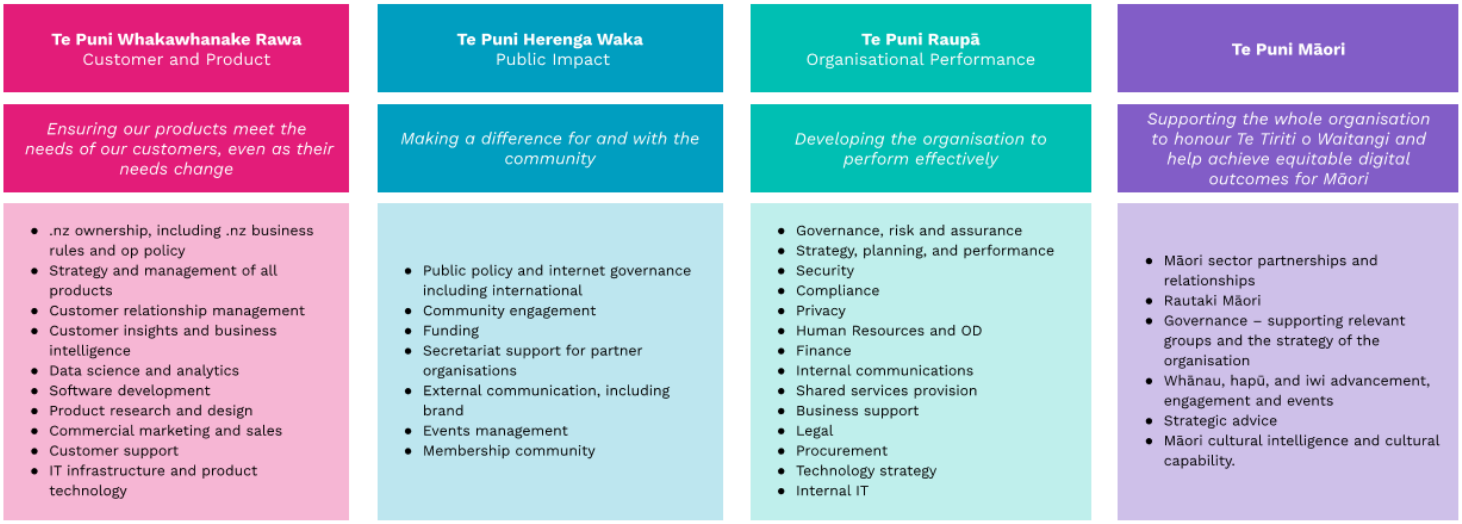
(We believe this process is technically possible, but it may be operationally infeasible to make the process "safe enough for break glass usage".)

Appendices

Appendix I – InternetNZ Organisational Structure

Taken from the InternetNZ 2022 decision document.





Appendix II – DNSViz diagram references

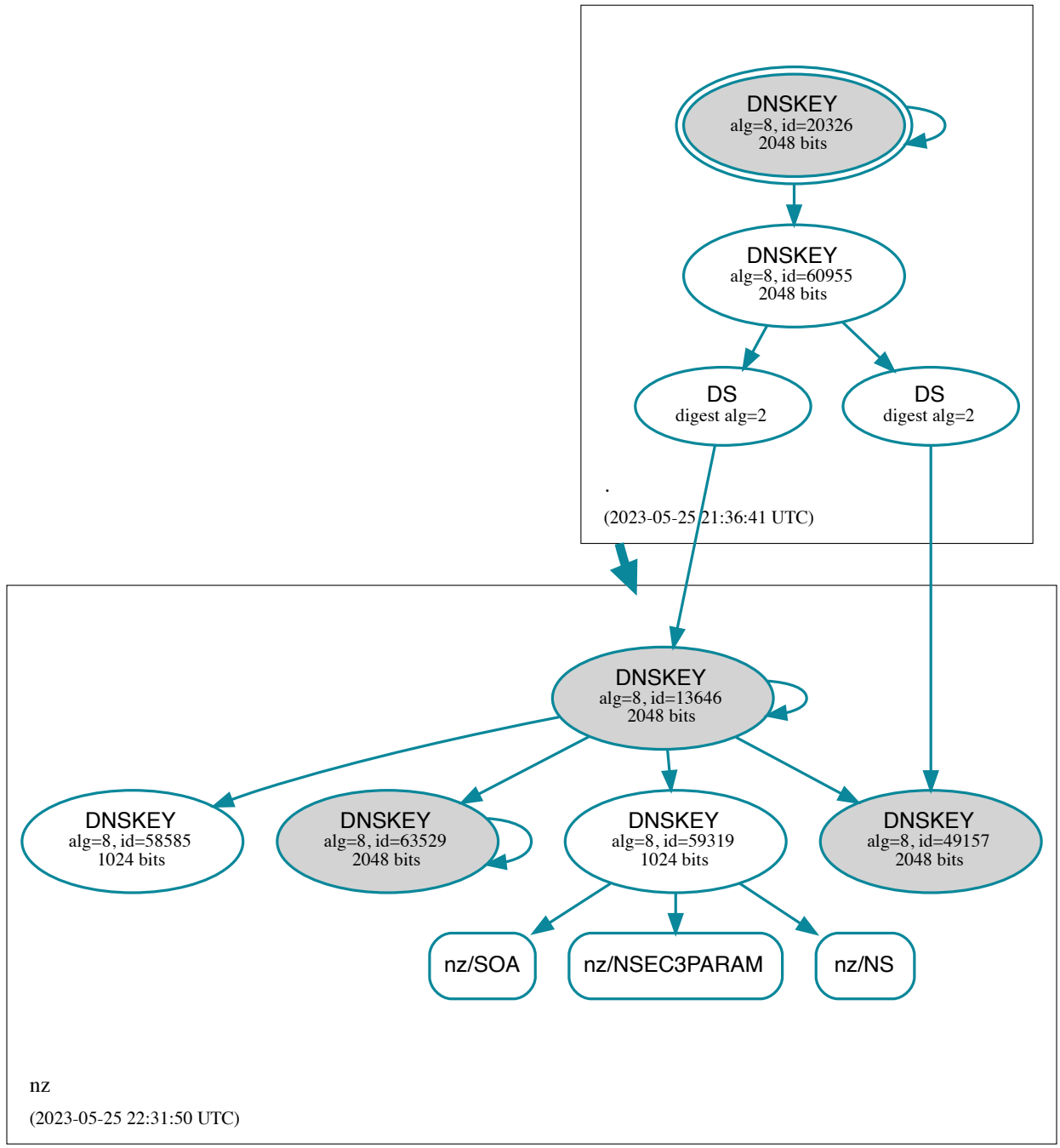
DNSViz is an online tool that can visualise DNS information, including DNSSEC record structures. It stores the DNS analysis that was done by people in the past, so provides a way of looking back at older DNS structures (near the root of the DNS) *when someone thought to run an analysis at the time*. While the past information is necessarily incomplete the details captured by DNSViz were invaluable in determining which DNSSEC keys (KSK and ZSK) were referenced by which DS/DNSKEY records at the known times in the past.

This appendix captures vector graphics from DNSViz for the .nz TLD and some key second level domains at some key points in their transition (mostly referenced in the report or timeline). It is intended as a "quick reference" for those reading the report, and a "better than nothing" archive if the DNSViz information is no longer available. Interested readers are encouraged to click through the links to the DNSViz site as a considerable amount of additional information is available in the interactive view through hover-over popups; but the key "key ID" information is captured in the exported SVG files below.

.nz top level domain

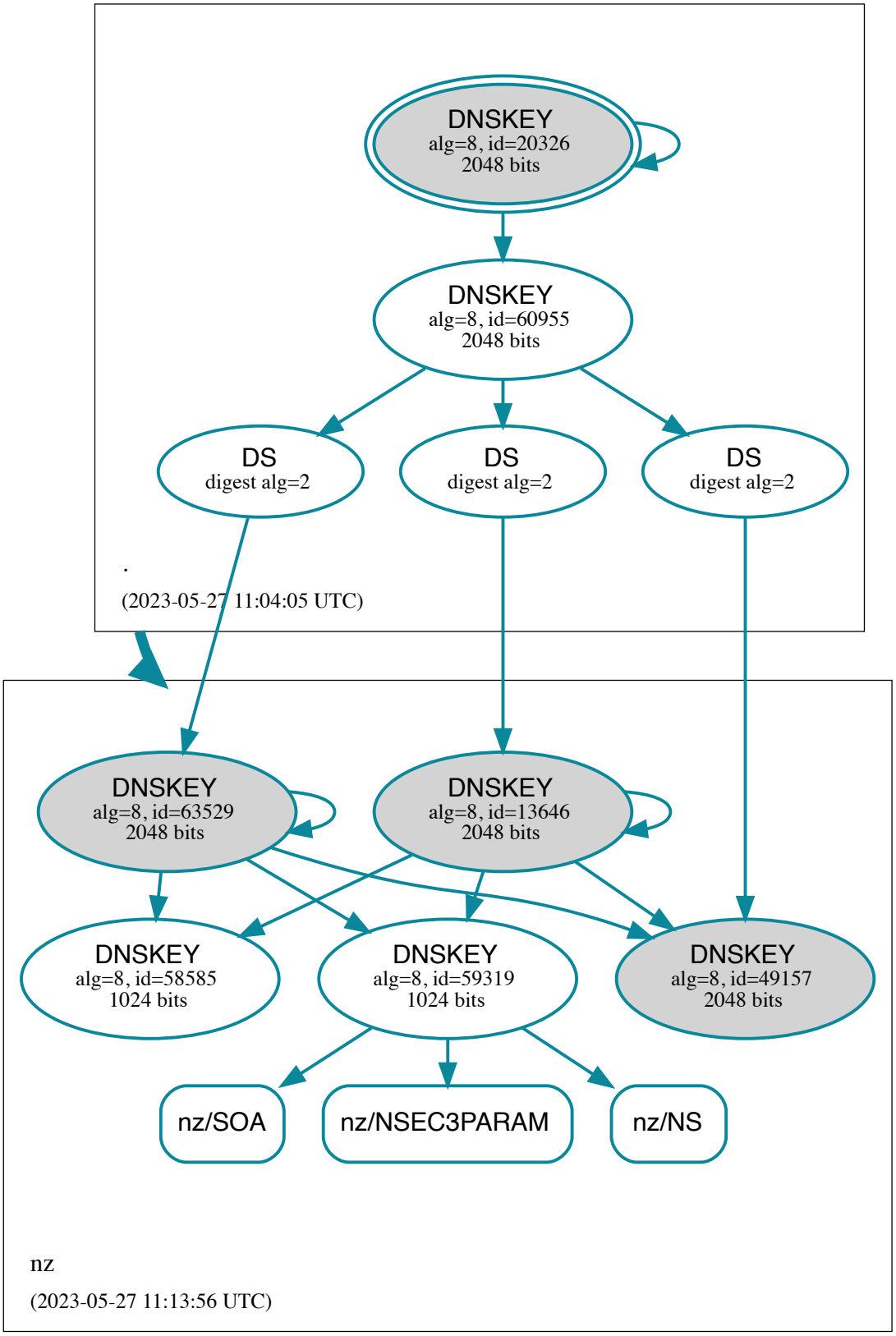
.nz TLD: 2023-05-26 10:31:50 NZST

From https://dnsviz.net/d/nz/ZG_h1g/dnssec/



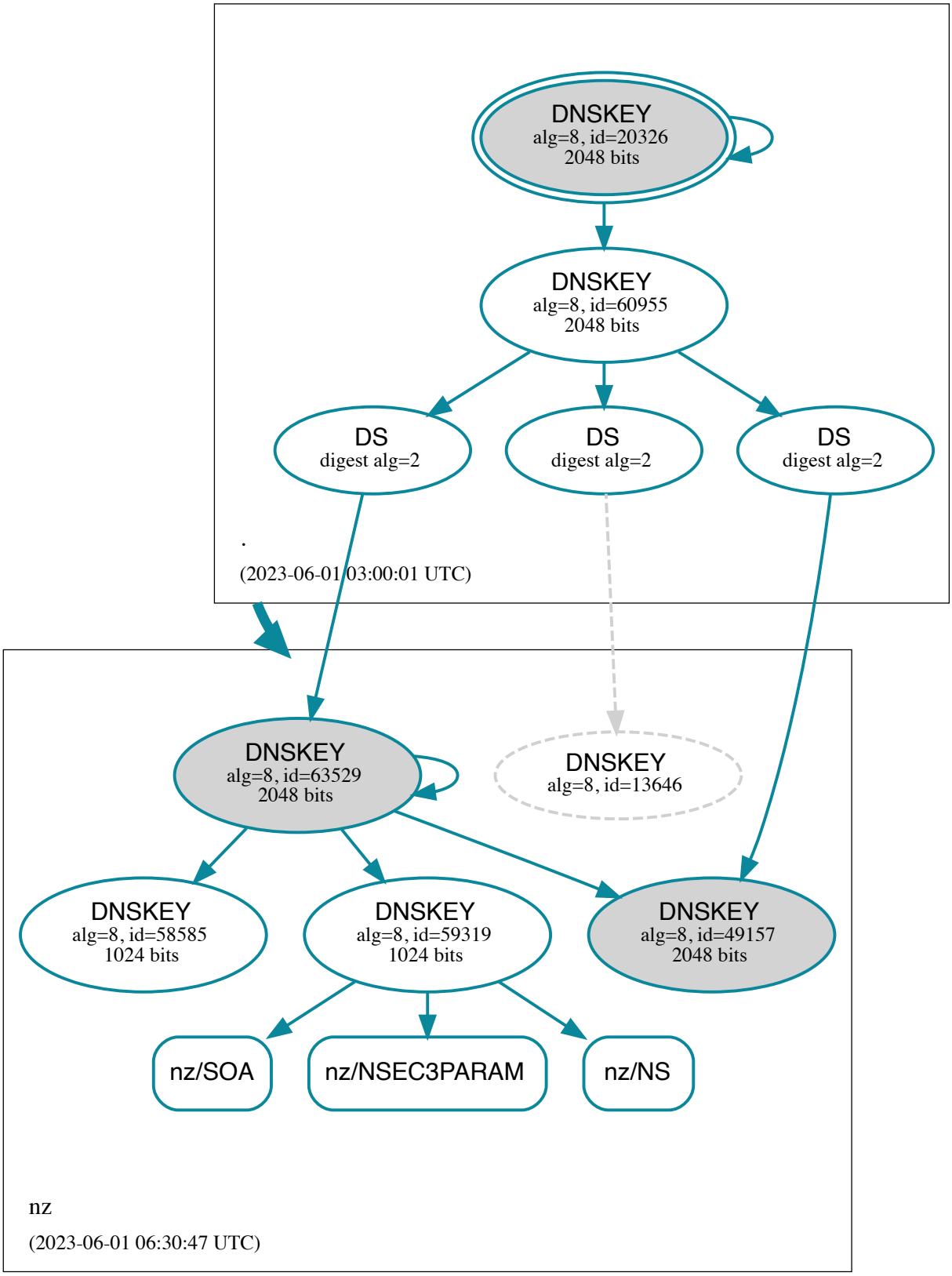
.nz TLD: 2023-05-27 23:13:56 NZST

From https://dnsviz.net/d/nz/ZHHl9A/dnssec/



.nz TLD: 2023-06-01 18:30:47 NZST

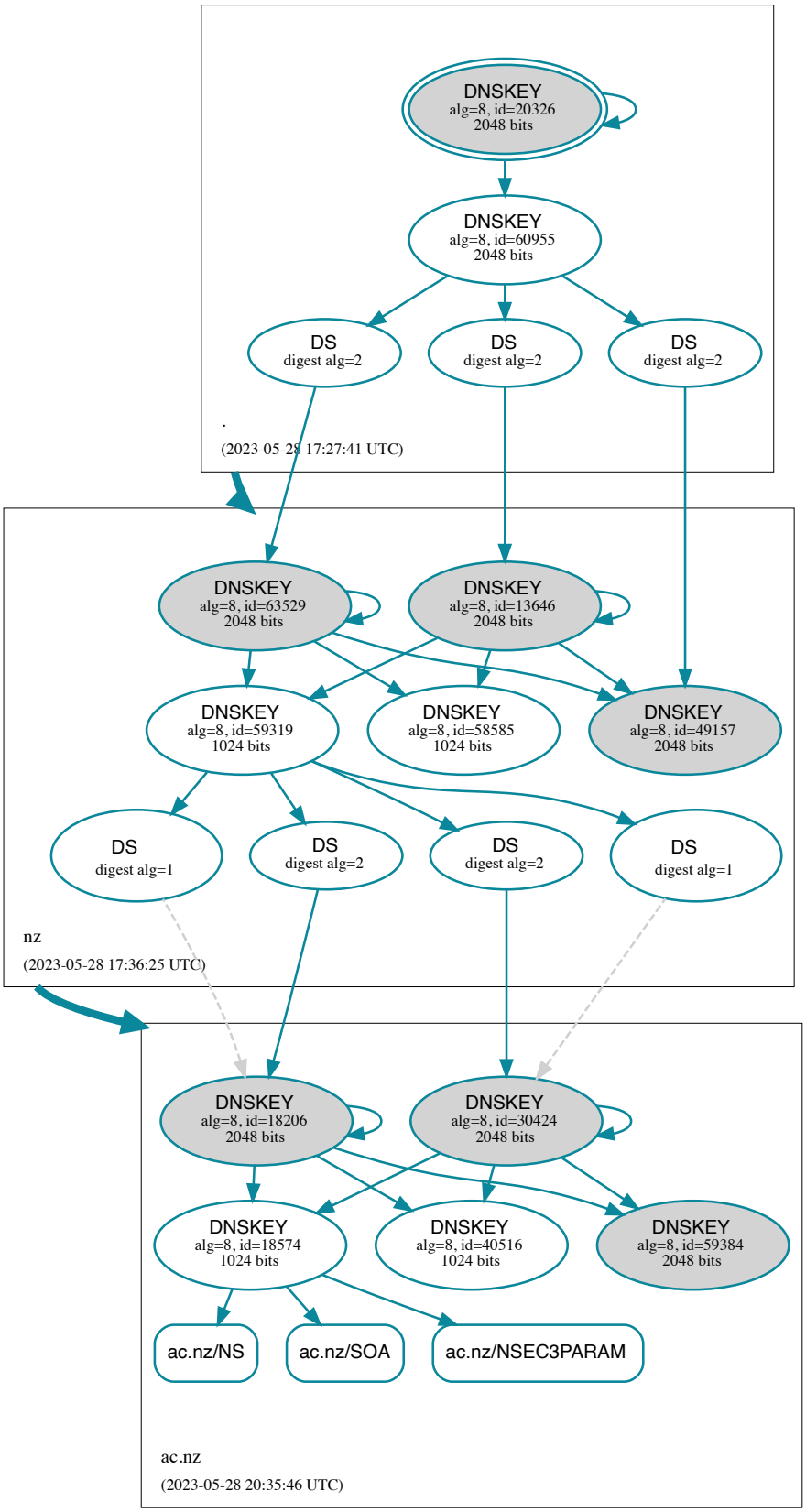
From https://dnsviz.net/d/nz/ZHg7Fw/dnssec/



ac.nz second level domain

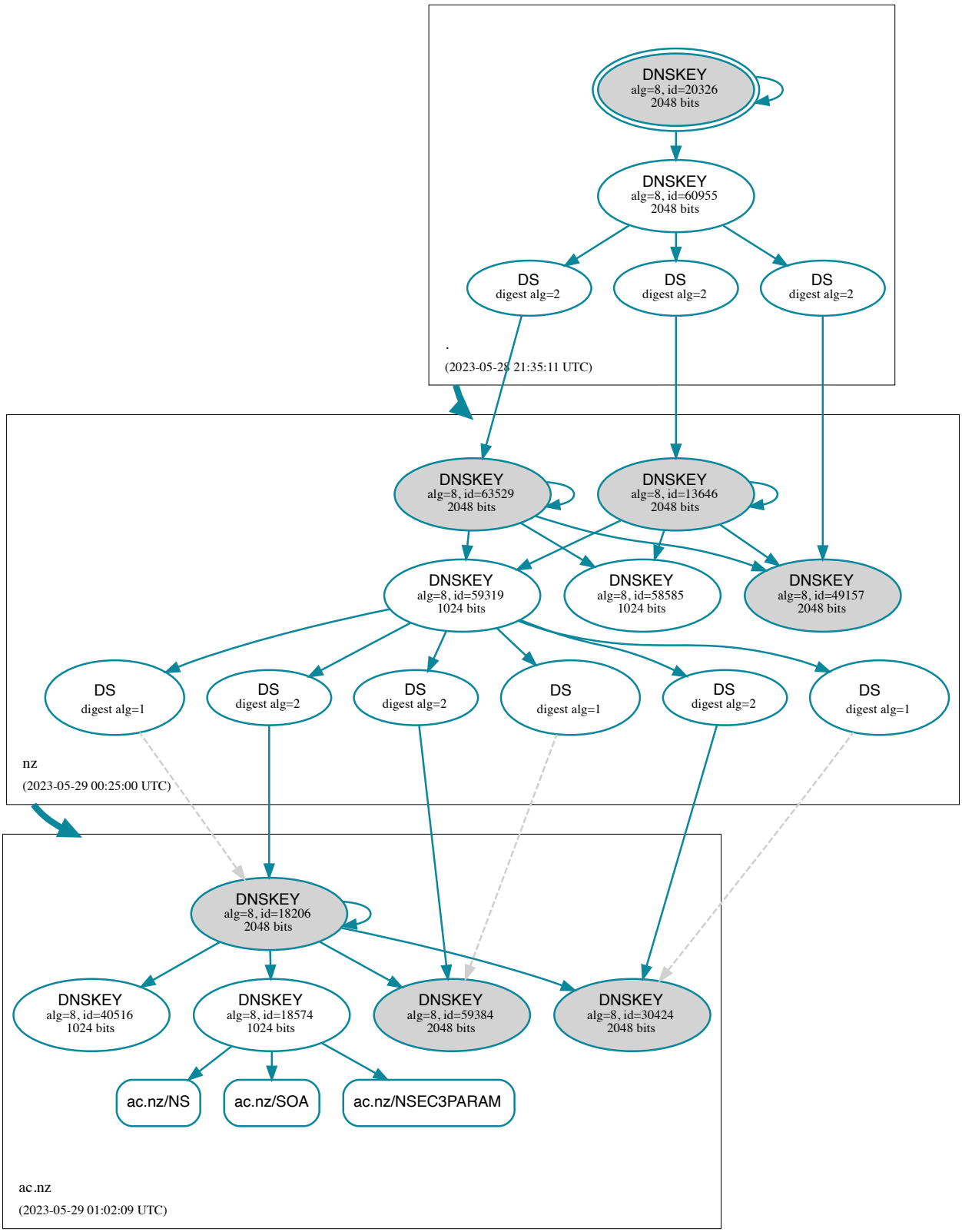
ac.nz: 2023-05-29 08:35:46 NZST

From https://dnsviz.net/d/ac.nz/ZHO7Ig/dnssec/



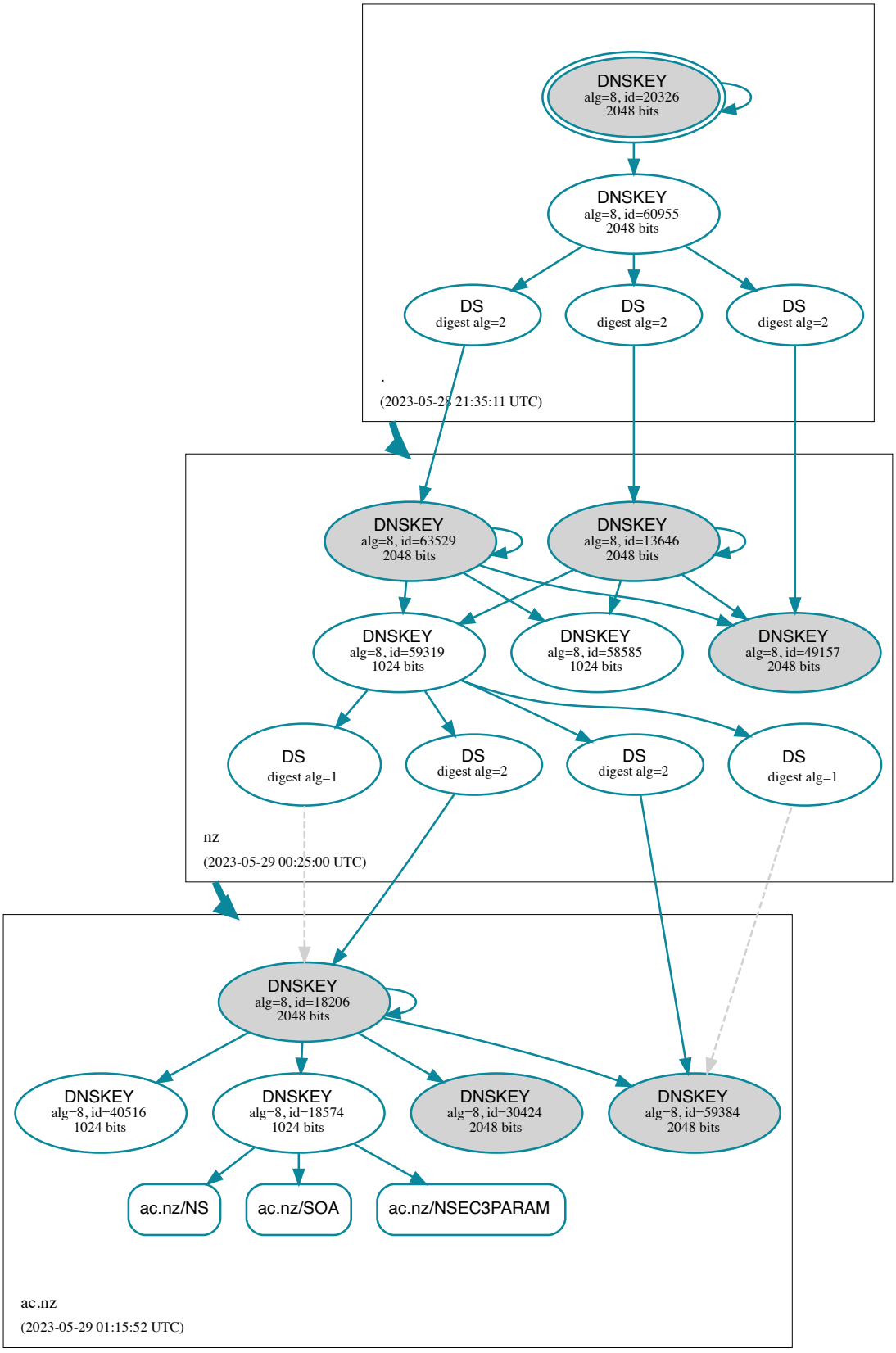
ac.nz: 2023-05-29 13:02:09 NZST

From https://dnsviz.net/d/ac.nz/ZHP5kQ/dnssec/



ac.nz: 2023-05-29 13:15:52 NZST

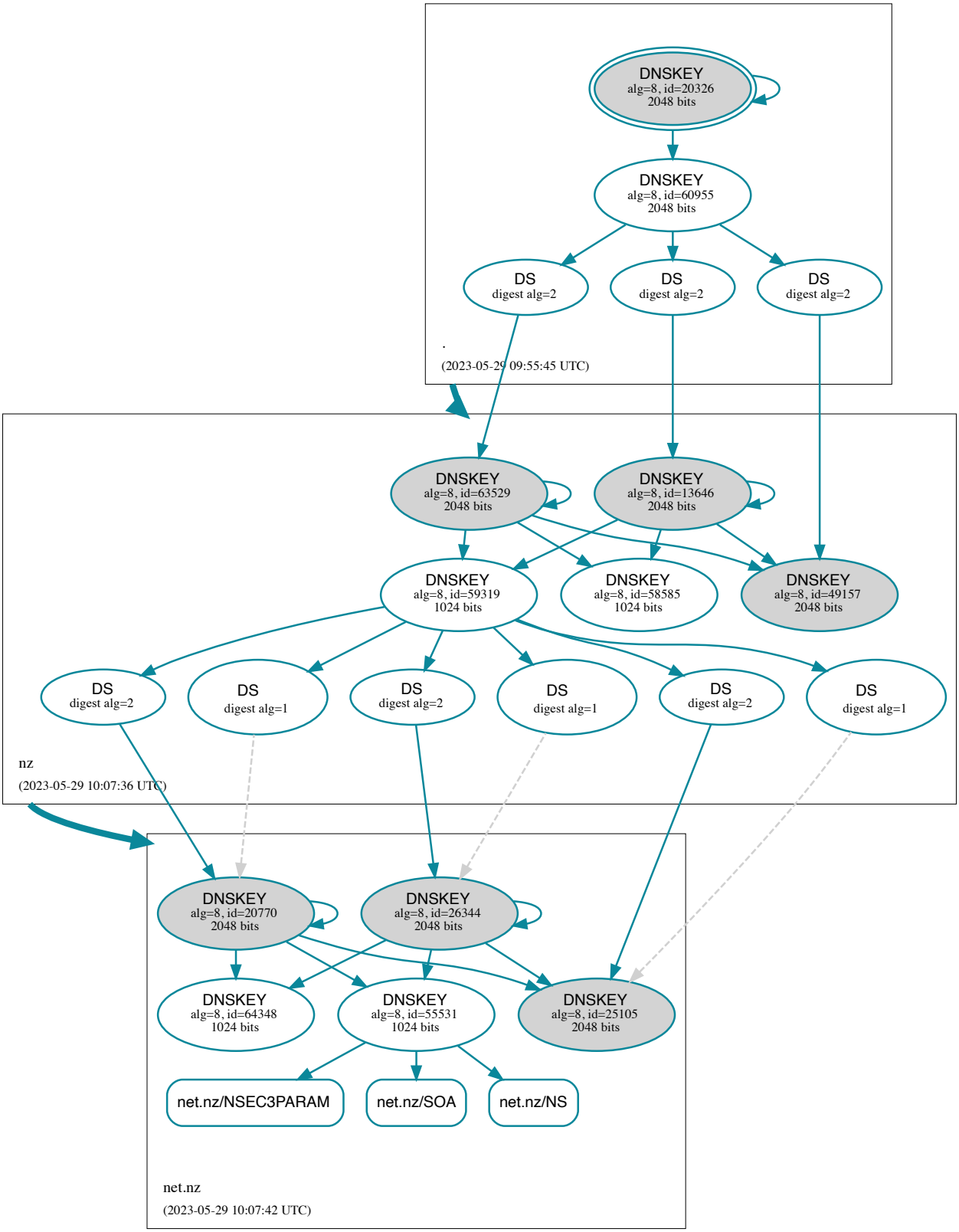
From https://dnsviz.net/d/ac.nz/ZHP8yA/dnssec/



net.nz second level domain

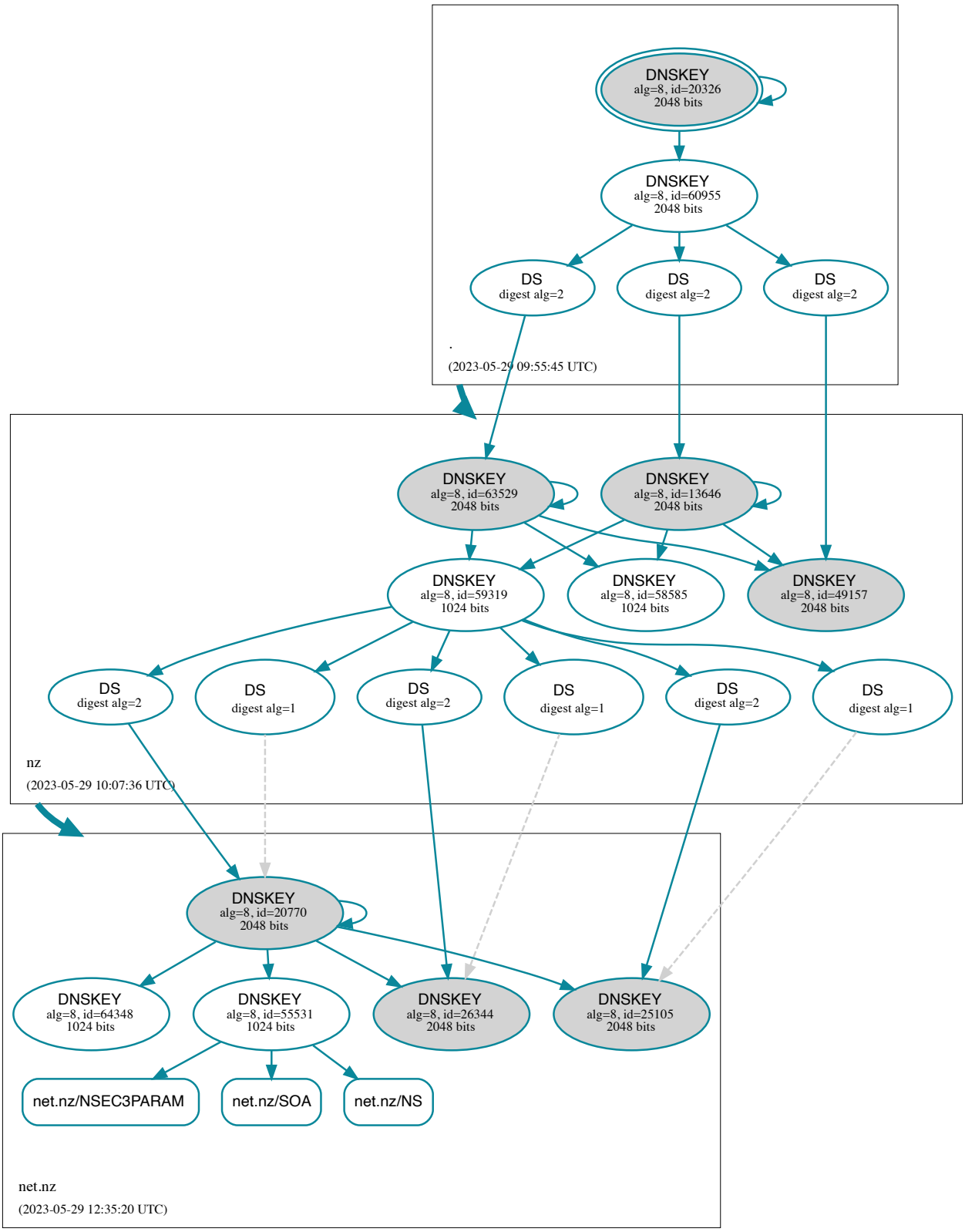
net.nz: 2023-05-29 22:07:42 NZST

From https://dnsviz.net/d/net.nz/ZHR5bg/dnssec/



net.nz: 2023-05-30 00:35:20 NZST

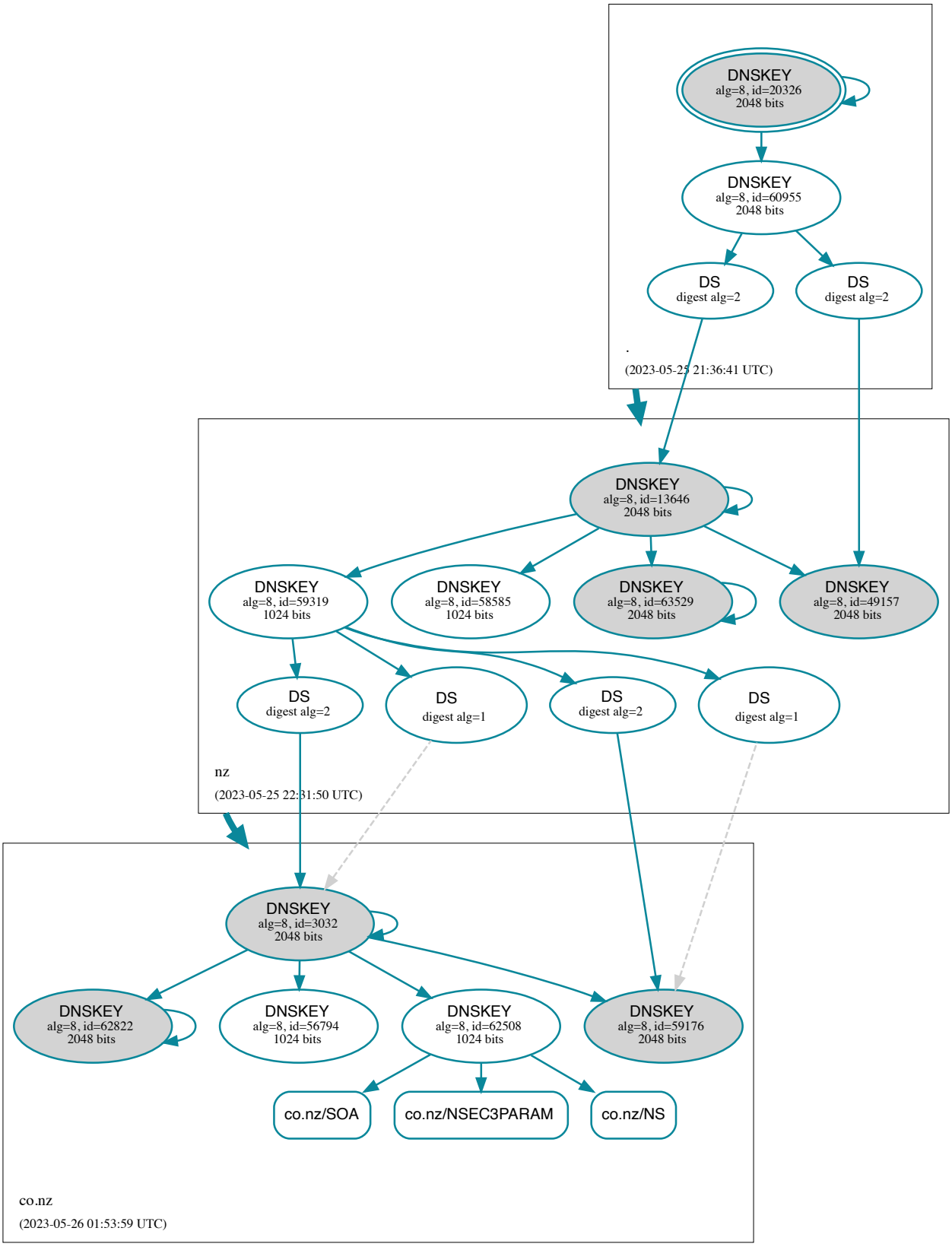
From https://dnsviz.net/d/net.nz/ZHScCA/dnssec/



co.nz second level domain

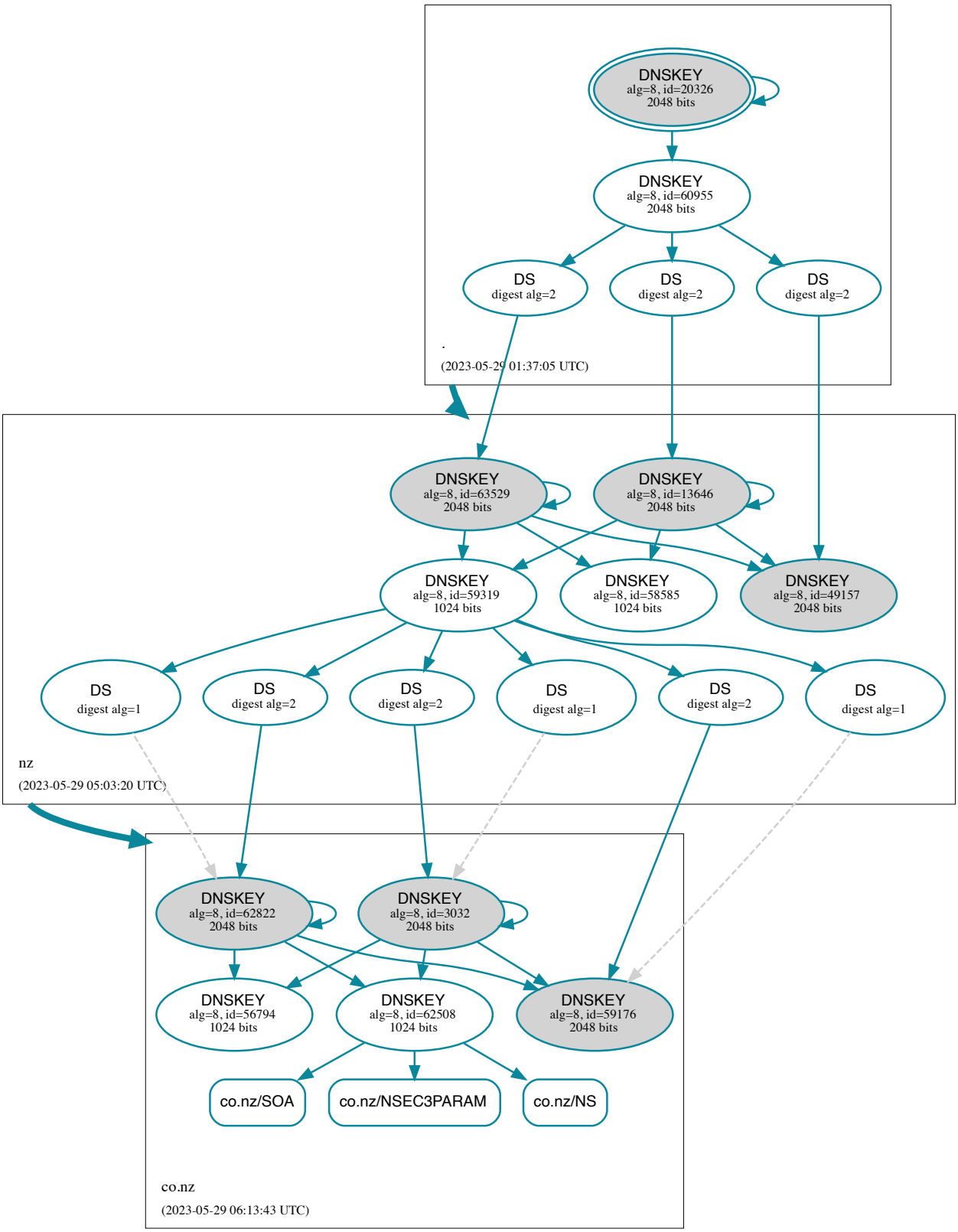
co.nz: 2023-05-26 13:53:59 NZST

From https://dnsviz.net/d/co.nz/ZHARNw/dnssec/



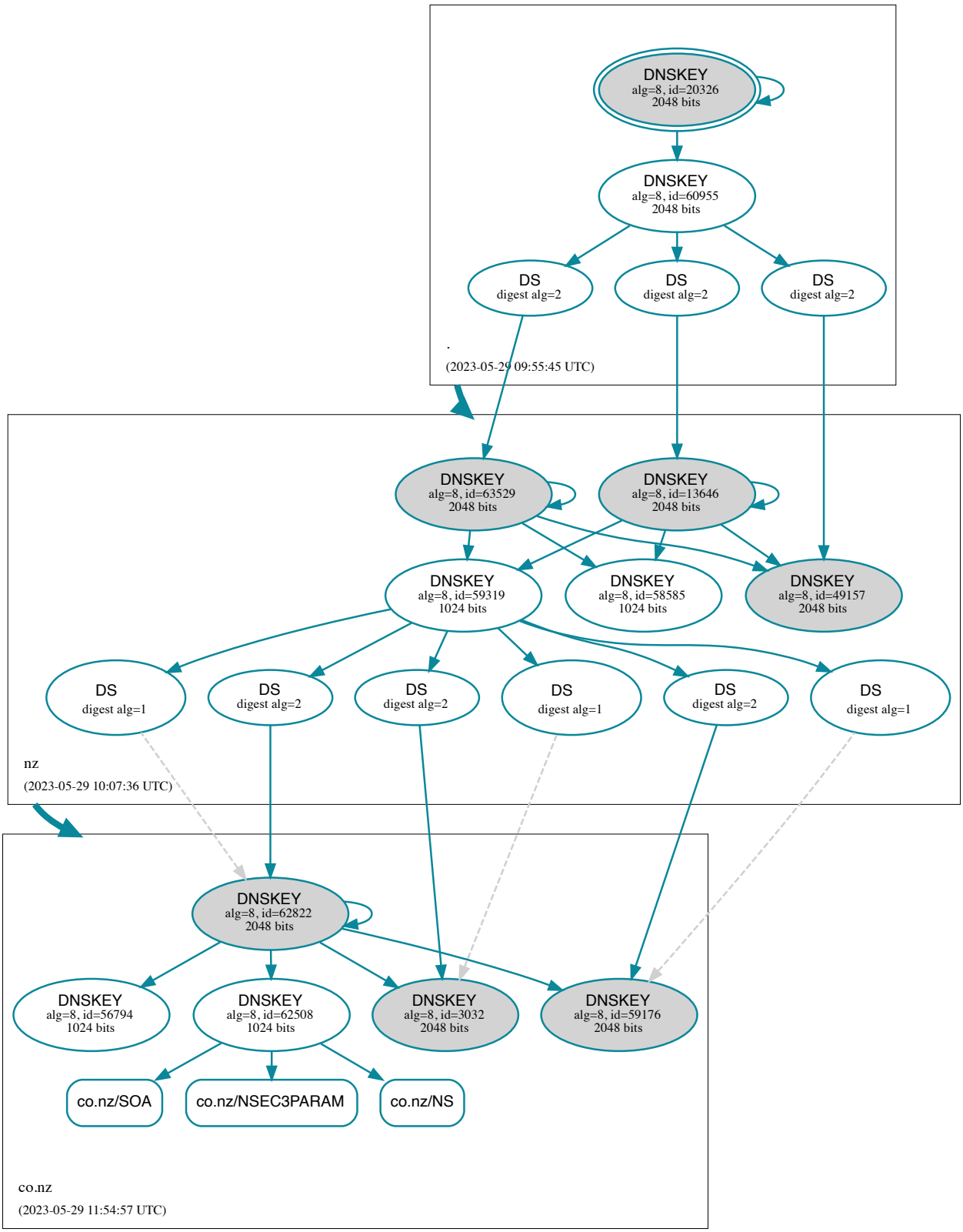
co.nz: 2023-05-29 18:13:43 NZST

From https://dnsviz.net/d/co.nz/ZHRClw/dnssec/



co.nz: 2023-05-29 23:54:57 NZST

From https://dnsviz.net/d/co.nz/ZHSSkQ/dnssec/



co.nz: 2023-06-01 18:36:33 NZST

From https://dnsviz.net/d/co.nz/ZHg8cQ/dnssec/