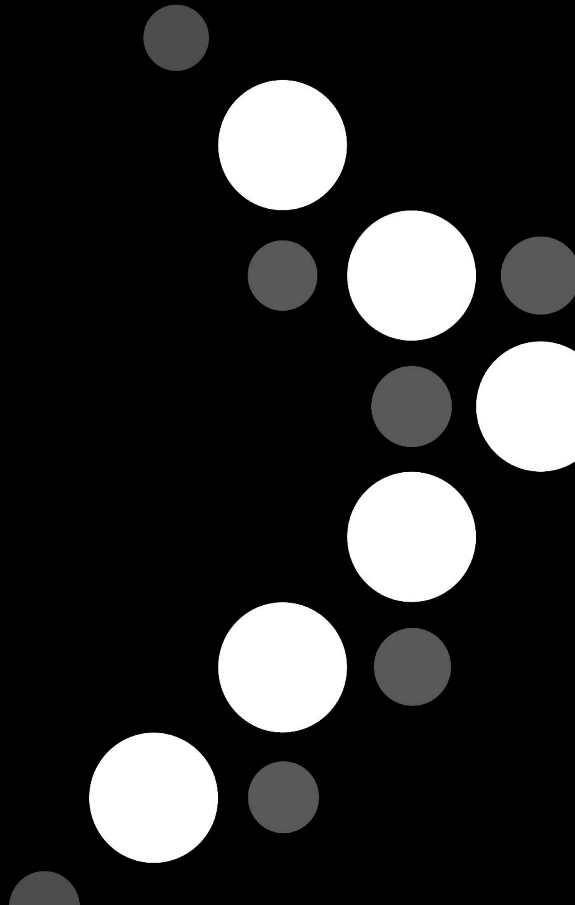
Increasing DNSSEC visibility in a multi-signer environment using fake-root stack

February, 2025

Felipe Agnelli Barbosa | InternetNZ

> Purpose

Requirements
Planning
Implementation
Usage
Future Work



-> **Anticipate**

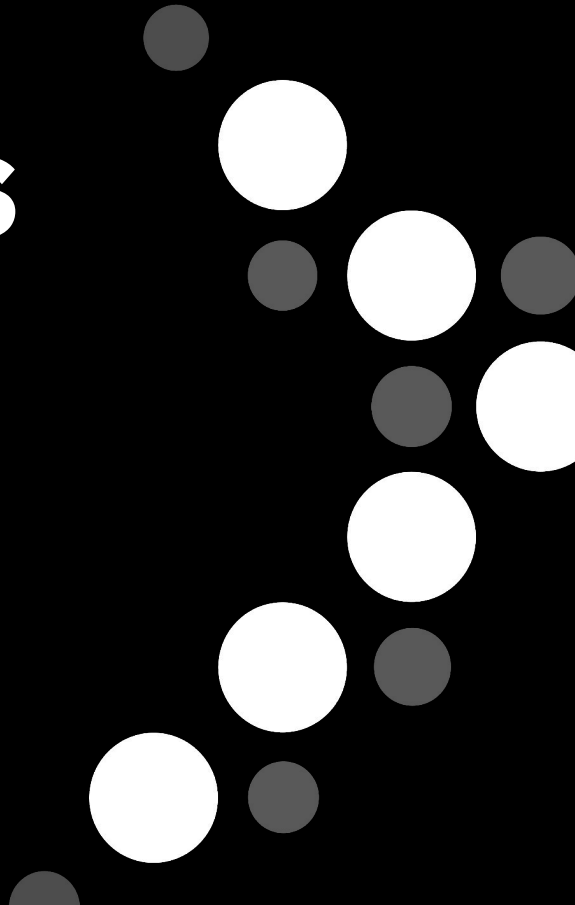
-> **Simulate**

-> **Visibility**

Purpose

> Requirements

Planning
Implementation
Usage
Future Work

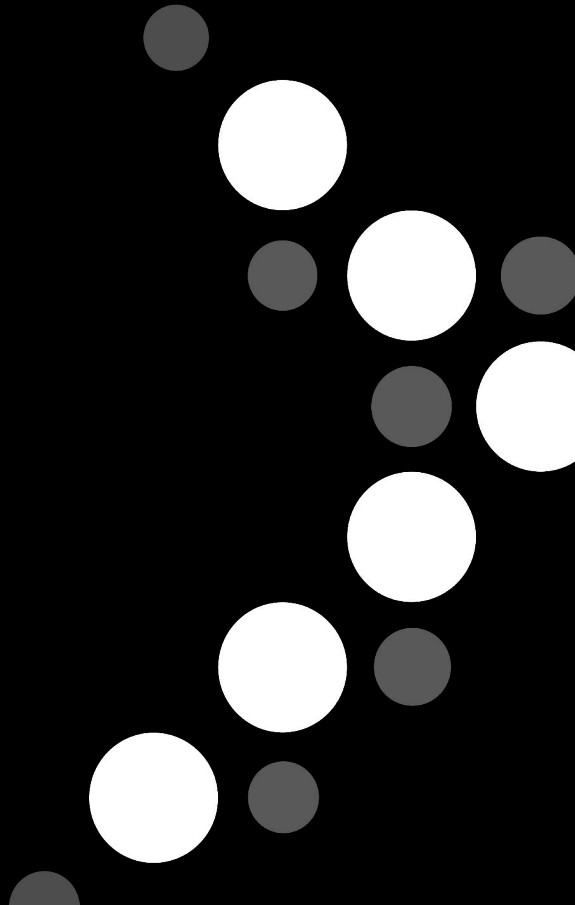


- Recursive perspective
- Use our data
- **+Ad** bit
- History
- Automated
- Presence in every environment of each site

Purpose
Requirements

> Planning

Implementation
Usage
Future Work



One box solution | Containers

- **.(dot) auth server**
- **.nz auth server**
- **recursive server**
- **dnsviz**
- **nginx**

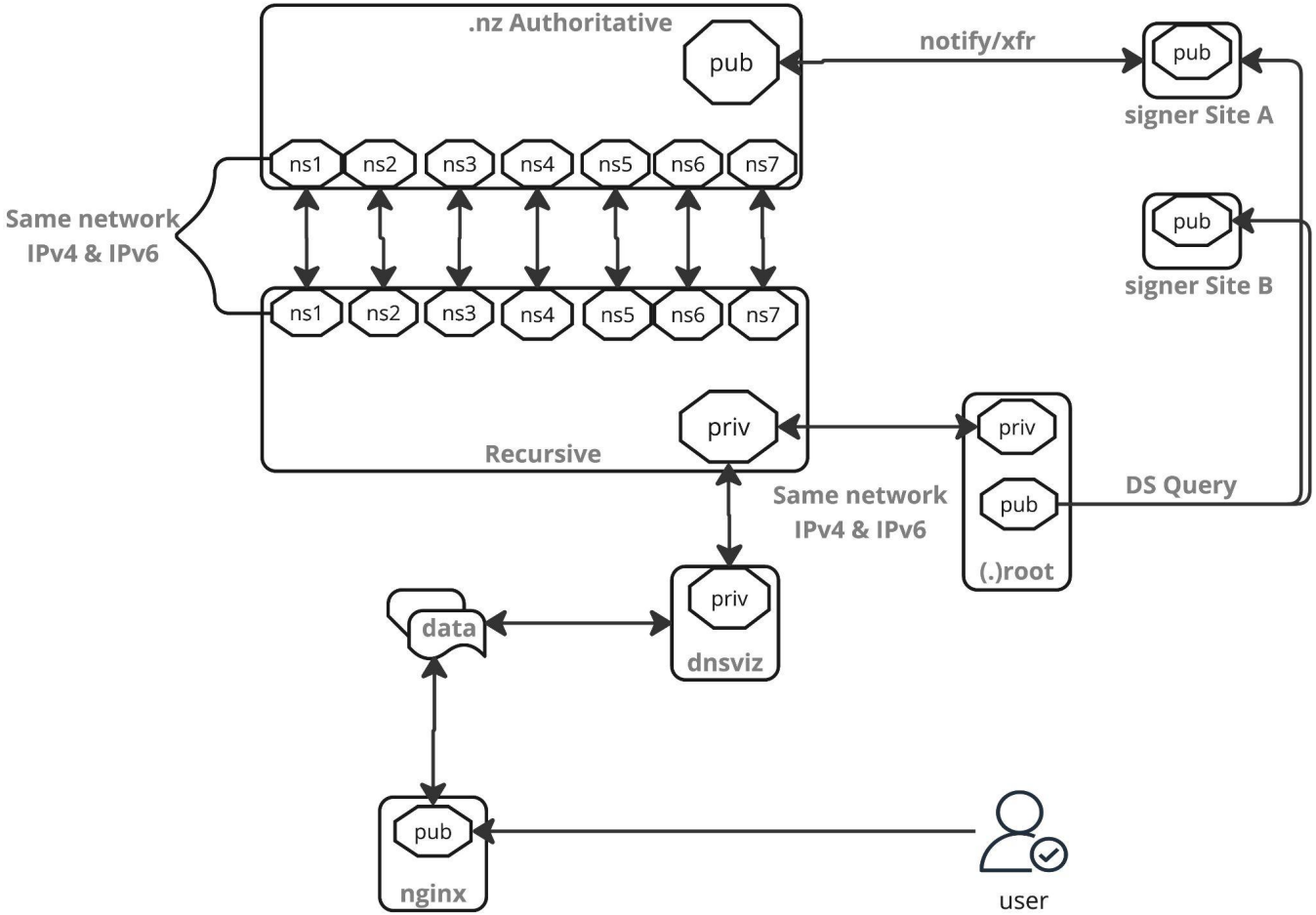
Monitoring of monitoring(Quis custodiet ipsos custodes)

- .(dot) Auth Server + .nz Auth Server
  - Bind
  - DNS communication with real signers
  - Automatic resign
  - /24(IPv4) and /64(IPv6) networks
- Recursive Server
  - Unbound
  - Custom root.hints and root.key
  - Cache enabled
  - /24(IPv4) and /64(IPv6) networks

- DNSViz
  - CRON job
  - Custom root.key
  - Recursive server
  - Query, probe, graph, grok
- Nginx
  - HTML frontend

fake-root-stack

Network overview

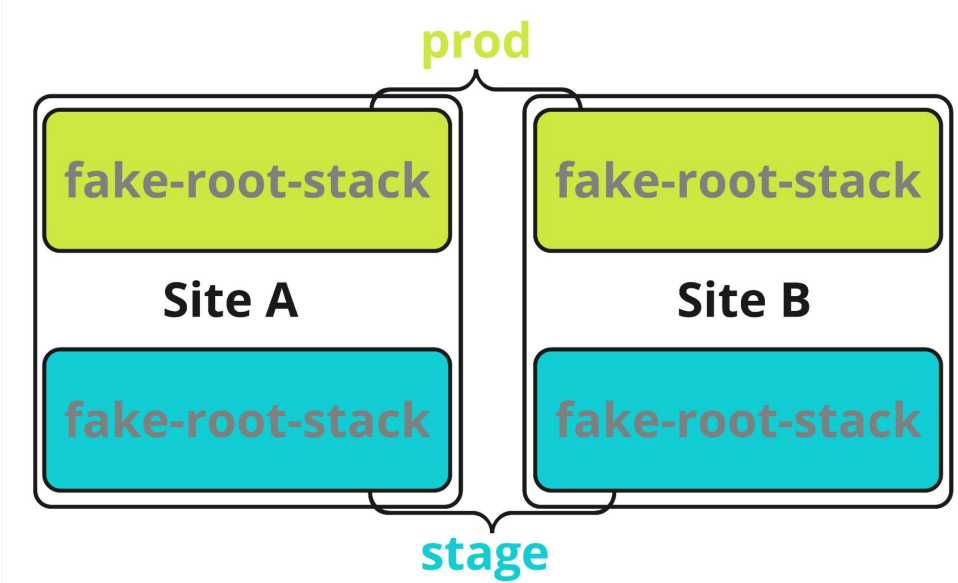


Purpose
Requirements
Planning

> Implementation

Usage
Future Work

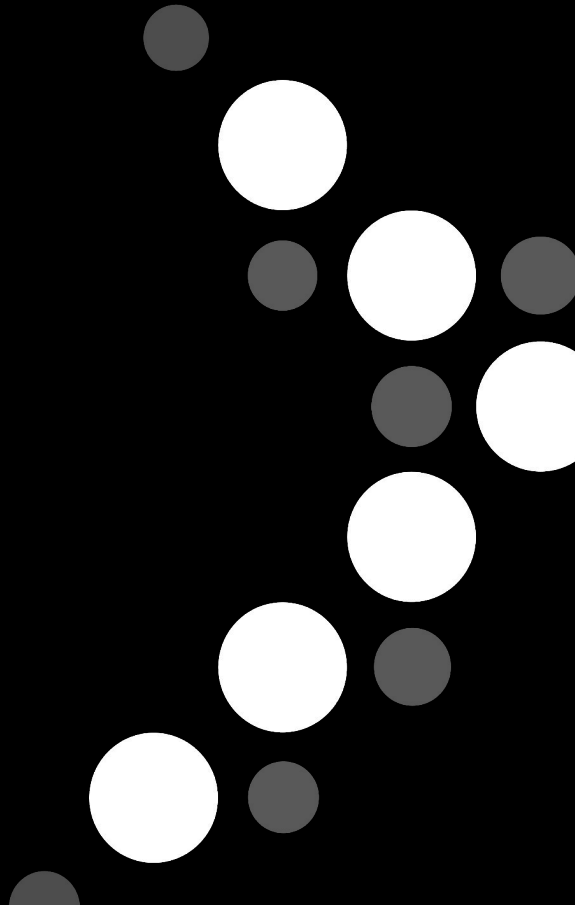
- Ubuntu VM
- Git+ansible
- 2 sites, 2 environments



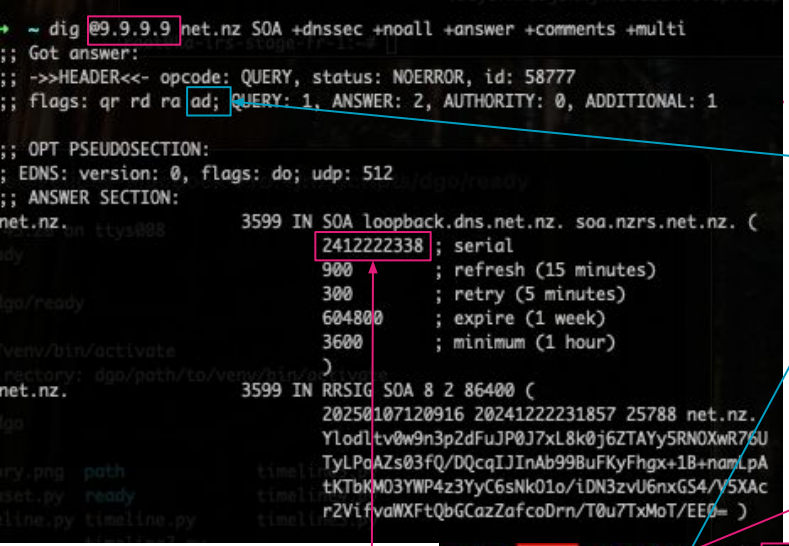
Purpose
Requirements
Planning
Implementation

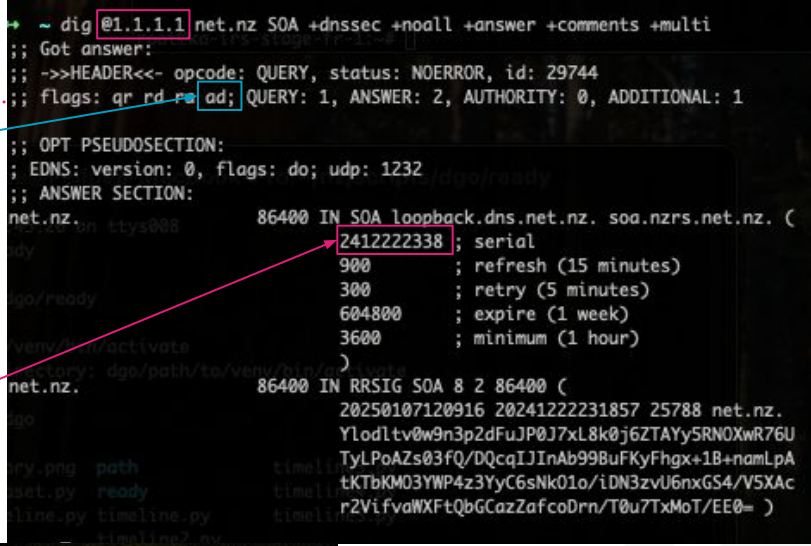
> Usage

Future Work

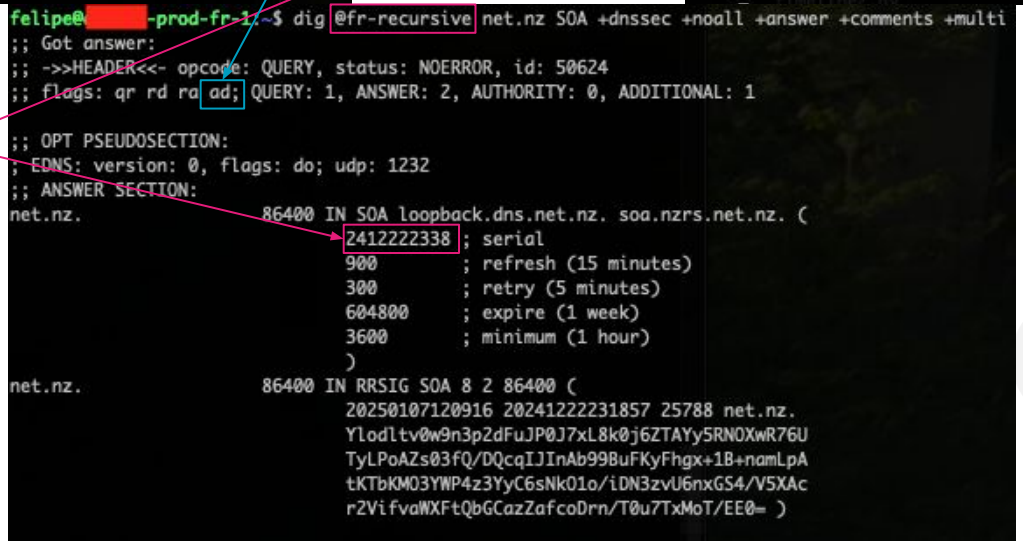


1. Health of the fake-roots
2. “Cut” the DNS communication
3. Guard-rail
4. **Active and Standby chains**





+ad Flag



Same Serial
2412222338

Tracing validation

```
$ dig @fr-root . dnskey +dnssec \
> +multi +noall +answer \
> | awk '$3 ~ /KSK/ { print "KSK:"$11}'
KSK:47777
$ dig @fr-root . dnskey +dnssec \
> +multi +noall +answer \
> | awk '$3 ~ /ZSK/ { print "ZSK:"$11}'
ZSK:29136
```

```
$ drill -QTD net.nz SOA -k root.key -r root-alt.hints
;; Number of trusted keys: 2
;; Domain: .
[T] . 300 IN DNSKEY 257 3 8 ;{id = 47777 (ksk), size = 2048b}
. 300 IN DNSKEY 256 3 8 ;{id = 29136 (zsk), size = 1024b}
[T] nz. 300 IN DS 39170 8 2 adb8214ccf90d5a927e27197cb6dae06682358ab
25735807c3cd7cd95baa11f7
nz. 300 IN DS 934 8 2 9d58f1627c135043f2cb12df20545c53f02f1bb78e7ed5
62c802084dfb672e2e
;; Domain: nz.
[T] nz. 3600 IN DNSKEY 257 3 8 ;{id = 39170 (ksk), size = 2048b}
nz. 3600 IN DNSKEY 256 3 8 ;{id = 10011 (zsk), size = 1024b}
nz. 3600 IN DNSKEY 256 3 8 ;{id = 51301 (zsk), size = 1024b}
nz. 3600 IN DNSKEY 257 3 8 ;{id = 934 (ksk), size = 2048b}
[T] net.nz. 86400 IN DS 24542 8 2 b7949d6e91c518825e70ce405061d9bc1c
abbc7fac25b97d532188172f63928e
net.nz. 86400 IN DS 16159 8 2 0254b68a7f2d29c9fb5c1be1aad61b7760b5ce
f49fc63c66ed33de38b0d380a1
;; Domain: net.nz.
[T] net.nz. 3600 IN DNSKEY 257 3 8 ;{id = 16159 (ksk), size = 2048b}
net.nz. 3600 IN DNSKEY 256 3 8 ;{id = 39709 (zsk), size = 1024b}
net.nz. 3600 IN DNSKEY 256 3 8 ;{id = 22990 (zsk), size = 1024b}
net.nz. 3600 IN DNSKEY 257 3 8 ;{id = 24542 (ksk), size = 2048b}
[T] net.nz.      86400   IN      SOA     loopback.dns.net.nz. soa.nzr
s.net.nz. 2501291754 900 300 604800 3600
;;[S] self sig OK; [B] bogus; [T] trusted
```

DNSViz [redacted]-prod-fr-1

Last Updated: 20250128T175501Z

History

- Last Run
- 20250128T175501Z
- 20250128T174002Z
- 20250128T172502Z
- 20250128T171001Z
- 20250128T165501Z
- 20250128T164001Z
- 20250128T162501Z
- 20250128T161001Z
- 20250128T155501Z
- 20250128T154002Z
- 20250128T152502Z
- 20250128T151002Z
- 20250128T145502Z
- 20250128T144001Z
- 20250128T142502Z
- 20250128T141001Z
- 20250128T135502Z
- 20250128T134002Z
- 20250128T132501Z
- 20250128T131001Z
- 20250128T125502Z
- 20250128T124001Z
- 20250128T122502Z
- 20250128T121001Z
- 20250128T115502Z
- 20250128T114001Z
- 20250128T112502Z
- 20250128T111001Z
- 20250128T105501Z
- 20250128T104002Z

[redacted]-prod-fr-1 20250128T165501Z

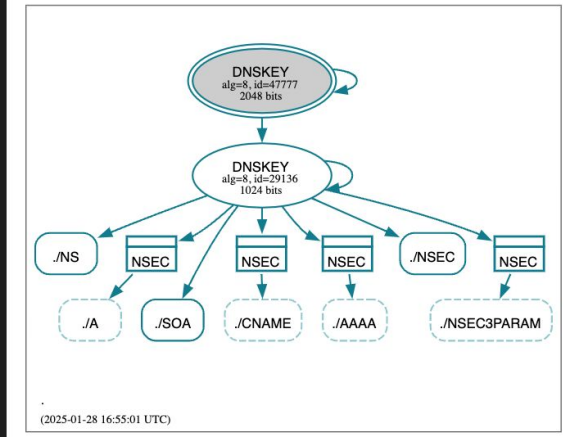
History | Combined TXT | Combined GROK | DNSViz Help

. [root] nz ac co cri geek gen govt health iwi kiwi maori mil net org parliament school

. [root]

TXT HTML

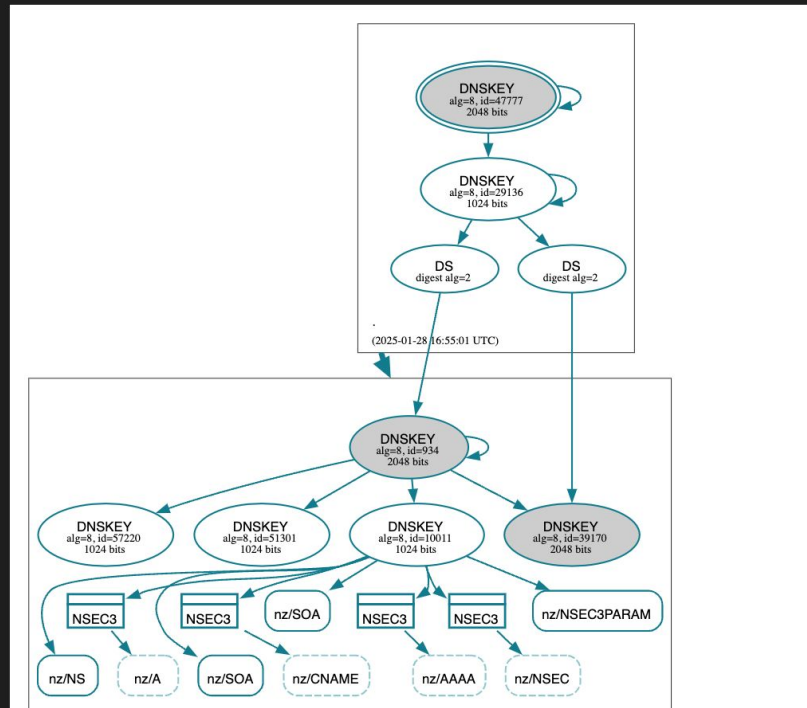
```
. [.]
  [.]  DNSKEY: 8/29136/256 [.], 8/47777/257 [.]
  [.]    RRSIG: ./8/29136 (2025-01-27 - 2025-02-26) [.]
  [.]    RRSIG: ./8/47777 (2025-01-27 - 2025-02-26) [.]
  [.]  A: NODATA
  [.]    SOA: ns. username. 1737974103 300 100 14400 60
  [.]      RRSIG: ./8/29136 (2025-01-27 - 2025-02-26) [.]
  [.]    PROOF:  [.]
  [.]      NSEC: . ns. NS SOA RRSIG NSEC DNSKEY
  [.]        RRSIG: ./8/29136 (2025-01-27 - 2025-02-26) [.]
```



nz

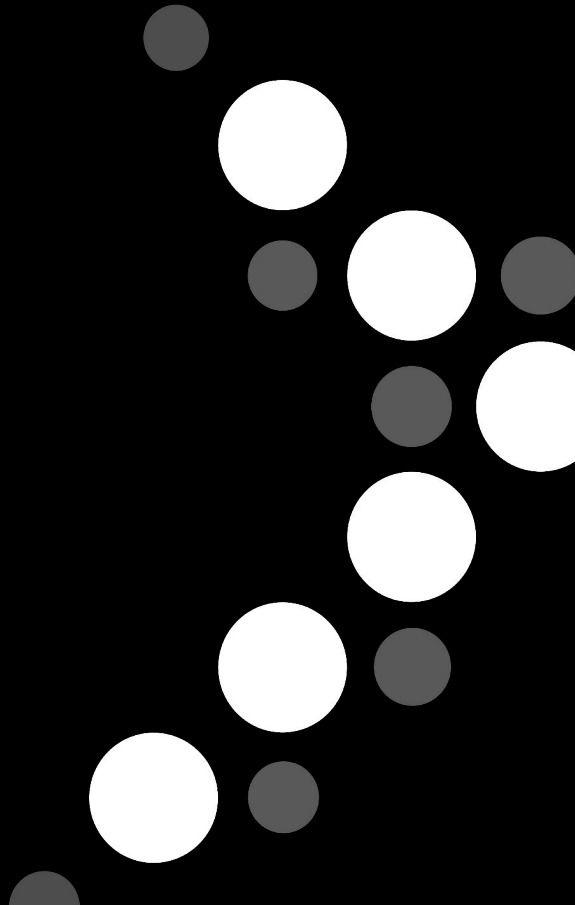
TXT HTML GROK

```
. [.]
  [.]  DNSKEY: 8/29136/256 [.], 8/47777/257 [.]
  [.]    RRSIG: ./8/29136 (2025-01-27 - 2025-02-26) [.]
  [.]    RRSIG: ./8/47777 (2025-01-27 - 2025-02-26) [.]
nz [.] [.]
  [.]  DS: 8/934/2 [.], 8/39170/2 [.]
  [.]    RRSIG: ./8/29136 (2025-01-27 - 2025-02-26) [.]
  [.]  DNSKEY: 8/10011/256 [.], 8/934/257 [.], 8/39170/257 [.], 8/51301/256 [.], 8/57220/256 [.]
  [.]    RRSIG: nz/8/934 (2025-01-22 - 2025-02-03) [.]
  [.]  A: NODATA
  [.]    SOA: loopback.dns.net.nz. soa.nzrs.net.nz. 2501281609 900 300 604800 3600
  [.]      RRSIG: nz/8/10011 (2025-01-28 - 2025-02-11) [.]
  [.]    PROOF:  [.]
  [.]      NSEC3: 0G0AG3SOTJI48E67BOBBOS8TQ9C31AK9.nz. 1 1 0 - OGR4V2I2R8NOF34EK8DE5CHELF7SR99I NS SOA RRSIG DNSKEY NSEC3PARAM
  [.]        RRSIG: nz/8/10011 (2025-01-26 - 2025-02-02) [.]
```



Purpose
Requirements
Planning
Implementation
Usage

> Future Work



- Zonemaster
- New DNS vendors
- Real root servers
- Post-sign-hook
- DSC/DSP
- Proactive work

Thank you for your attention!

Contact | felipe@internetnz.net.nz