

Authenticating .govt.nz via DNSSEC

```
;; Received 673 bytes from 156.154.100.14#53(ns5.dns.net.nz) in 142 ms
ns2.dns.govt.nz.      28800  IN      A        202.160.117.18
dns.govt.nz.         28800  IN      NS       ns1.dns.govt.nz.
dns.govt.nz.         28800  IN      NS       ns2.dns.govt.nz.
;; Received 164 bytes from 202.160.117.18#53(ns2.dns.govt.nz) in 11 ms

mvg@ubuntu:~$ dig +trace www.dns.govt.nz

;<<> DiG 9.9.5-3-Ubuntu <<> +trace www.dns.govt.nz
;; global options: +cmd
.                5      IN      NS       j.root-servers.net.
.                5      IN      NS       l.root-servers.net.
.                5      IN      NS       h.root-servers.net.
.                5      IN      NS       a.root-servers.net.
.                5      IN      NS       i.root-servers.net.
.                5      IN      NS       k.root-servers.net.
.                5      IN      NS       m.root-servers.net.
.                5      IN      NS       g.root-servers.net.
.                5      IN      NS       d.root-servers.net.
.                5      IN      NS       c.root-servers.net.
.                5      IN      NS       e.root-servers.net.
.                5      IN      NS       f.root-servers.net.
.                5      IN      NS       n.root-servers.net.
.                5      IN      NS       o.root-servers.net.
.                5      IN      NS       r.root-servers.net.
.                5      IN      NS       s.root-servers.net.
.                5      IN      NS       t.root-servers.net.
.                5      IN      NS       u.root-servers.net.
.                5      IN      NS       v.root-servers.net.
.                5      IN      NS       w.root-servers.net.
.                5      IN      NS       x.root-servers.net.
.                5      IN      NS       y.root-servers.net.
.                5      IN      NS       z.root-servers.net.
.                5      IN      RRSIG  NS 8 0 518400 20141109170000 20141102160000 2 . . . hGh3Cuppy . . . a7nbbGFeIoZqGf50ZaiPuv2RK4kalV8GcdogySp6fyw OIDpi06mhbb6
jpoov8hC3JULQQMjg7ghXpYtL5ambAtniyVhGYFC7G6ow F7edl9G2zeQHEV722r1Q2EH/YHElgZUGm0GZLPeqz2yZnZ7mi7Favfn MEB=
;; Received 490 bytes from 192.168.30.1#53(e.root-servers.net) in 34 ms

ns.                86400  IN      NS       ns1.dns.govt.nz.
ns.                86400  IN      NS       ns2.dns.govt.nz.
ns.                172800 IN      NS       ns4.dns.net.nz.
ns.                172800 IN      NS       ns5.dns.net.nz.
ns.                172800 IN      NS       ns6.dns.net.nz.
ns.                172800 IN      NS       ns7.dns.net.nz.
ns.                86400  IN      DS       22552 8 2 1FC46E6DA263A530DF4A5EBC1C28D493C4C86F342E
ns.                86400  IN      DS       22552 8 2 4B78F4917376CD56BA71776F5AC76D928634FDB8F5F6DDBA87A46FB0 2DACP546
ns.                86400  IN      DS       22552 8 1 86400 20141109170000 20141102160000 22603 . Pxxw9ZmWgrVvLk83CZUdu8WzXhhB4I7vxj6v72jEgDqk/BtZ4zv/C8w 1B0yPQ7t/enki
NmaAIFAcasNufFmaiIw4qbcT0D/boCmuXhXrlx/y2Guge 6Hwx7go0JdYpfdpExlKXQgcDPR263FLMuZIEBz2nD9wNRLxUTT6uKd kXc=
;; Received 673 bytes from 192.203.230.10#53(e.root-servers.net) in 34 ms

dns.govt.nz.       86400  IN      NS       ns1.dns.govt.nz.
dns.govt.nz.       86400  IN      NS       ns2.dns.govt.nz.
oegndalsmjc8auhfmr8q5tjvbnubjg14.govt.nz. 3600  IN  NSSEC3 1 1 5 935FE2522E253BF8 77P83DTBVLPUd40PLBH759M8A9M60Q0M NS 60A RRSIG DNSKEY NSEC3PARAM
oegndalsmjc8auhfmr8q5tjvbnubjg14.govt.nz. 3600  IN  RRSIG NSSEC3 8 3 3600 20141108161325 20141030224510 45066 govt.nz. SRLP2B8dgyS/LSRXfmlkRbrva2leakGSSL6VC7PotpDmangWof0kUw
xm6 dtwanH+W*2iNqbxjD1a8h+4SFFaIVjUheG3iW0+3+xsKWFf0c4pav9z IM4HfQrYG6eE2Nyb3KvdZVrvfYfG63nG5lxPSZKJnIKW19CaymQu0rCmn ua#
7tP83dtbvlpu40plbh759m8a9m60q0m.govt.nz. 3600  IN  NSSEC3 1 1 5 935FE2522E253BF8 OBQND8LJJC8AUHFJMR8Q57J7SVBNJUG14 TXT RRSIG
7tP83dtbvlpu40plbh759m8a9m60q0m.govt.nz. 3600  IN  NSSEC3 8 3 3600 20141108203648 20141030224510 45066 govt.nz. S8M1jg/gmqIG3Yo8bP2b7CCLtxgLJmAs7h80SaF8ed8RO0U2VfzQ
PxF DADiwi7oLjTgMdCHTgWbyGodE5+Ka8n516Tcw01lx9QR0ULKEZFc11 qBE8RdYOGAuaYh74AyAXoarm0/RitI3vUmqcv9i0w0BrdjXndGqkFapJ g7w=
;; Received 677 bytes from 202.46.187.130#53(ns2.dns.net.nz) in 28 ms

www.dns.govt.nz.   28800  IN      A        202.160.112.212
dns.govt.nz.      28800  IN      NS       ns2.dns.govt.nz.
dns.govt.nz.      28800  IN      NS       ns1.dns.govt.nz.
;; Received 184 bytes from 202.160.112.210#53(ns1.dns.govt.nz) in 3 ms
```

- Providing NZ Internet services since 2002.
- Operate the .govt.nz moderation, registrar and dns.govt.nz name-server platform for Department of Internal Affairs.
- Operate the .health.nz moderation and dns.health.nz name-server platform for Ministry of Health.
- Operate our own commercial registrar and ns{1,2,3}.modicagroup.com name-server platform.
- Mobile SMS messaging direct to all NZ carriers and world-wide.

- Technical design and implementation of a modern DNS moderation and management system.
- Assist with Hardware Security Module product selection, technical implementation of selected product.
- Existing modern DNS management system utilised for Modica DNS services.
- Extend existing platform to provide DNS moderation.
- Alter Modica's existing DNS management system to provide DNSSEC capabilities
- Integrate against a Two Factor Authentication system to ensure trust and integrity of DNS changes.

“You just need to change the IP address on your A record to what you want it to be”

“You just need to change the IP address on your A record to what you want it to be”



- DNS management is already difficult for many end-users tasked with responsibility.
- DNSSEC needs to be automatic, and require no end-user interaction.
- If you provide end-users choice over DNSSEC detail, it will confuse and alienate them. Uninformed bad choices will result - not end-user's fault - **DNS provider's fault.**

- Do not look to join the likes of:
 - cdc.gov
 - fbi.gov
 - irs.gov
 - nasa.gov
- All of these sites failed to automate their DNSSEC, then inevitably broke their domains.
- The lesson is well learnt now: Implement manual DNSSEC - you are planning to break your DNS.

- Do you need true hardware HSMs? Is SoftHSM appropriate?
- Take the time to evaluate true hardware HSM options well.
- Amazon CloudHSM - US\$5K up-front, between US\$1.88 - US\$2.24 per hour.
- Become operationally sound with your HSM infrastructure, practice - a lot. You'll thank yourself later.
- HSMs are a security appliance - aim to meet Common Criteria or NIST FIPS certification.
- Paranoid devices, features are a security risk. Expect weird and non-intuitive behaviours from an Internet engineering perspective.



- By design DNSSEC adds large records. Fail to implement DNS response rate limiting and you will become a DoS amplifier.
- Consider the DNSSEC policy decisions made by others in your DNS hierarchy. Root and .nz uses 1024-bit RSA ZSKs and 2048-bit RSA KSKs. It doesn't make sense to implement longer keys than this.
- Build in contingencies into key validity periods, how much key material you generate.
- Operational concerns like backups and monitoring remain important as ever.
- **You must always remember to ~~blow on the pie~~ automate your DNSSEC. Safer internet communities together!**