.govt.nz & DNSSEC

A short case study

05 Nov 2014

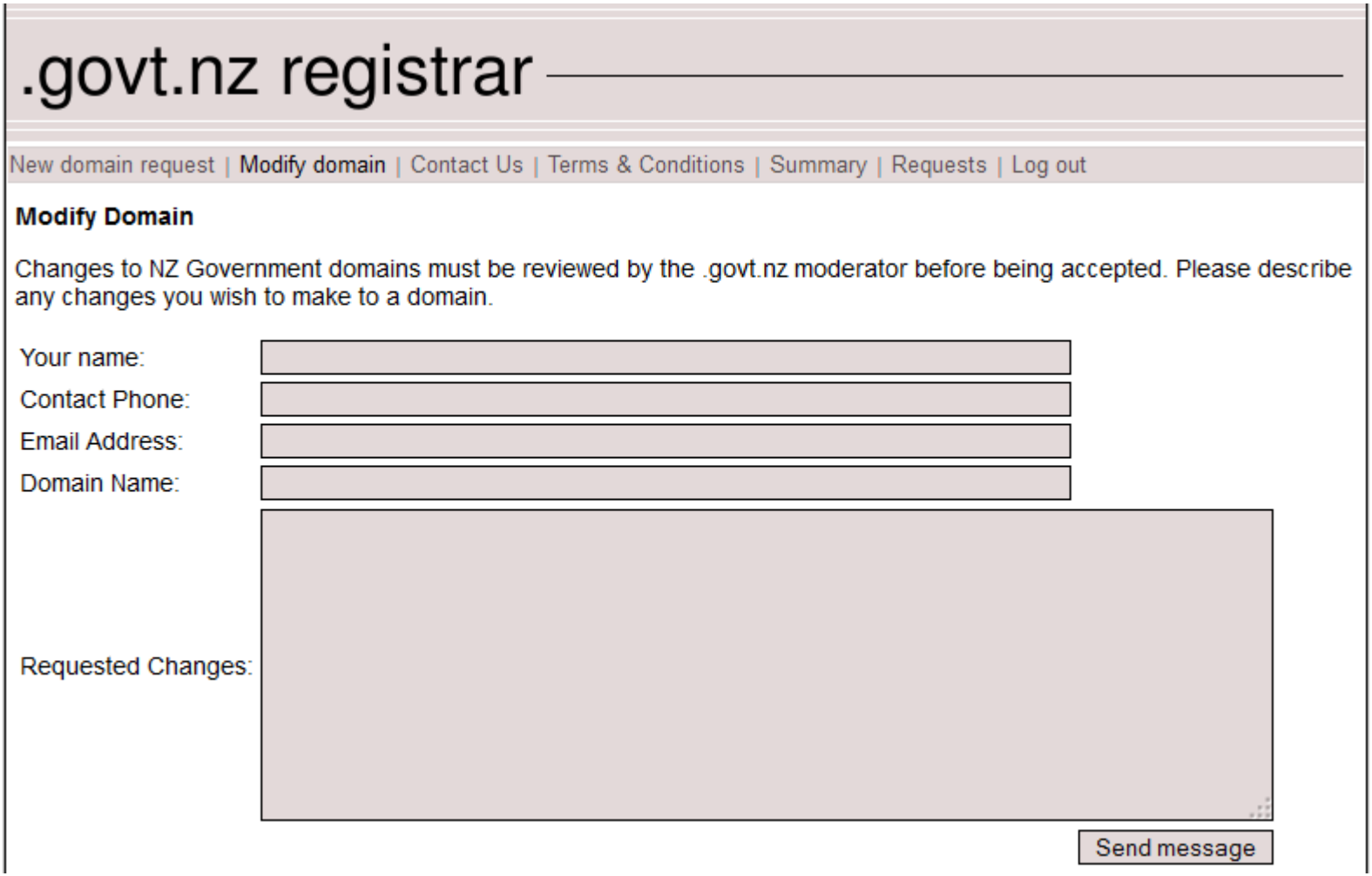
New Zealand Government

Current .govt.nz context

- Moderated domain
- 1,043 names (as of yesterday morning)
- Managed by Department of Internal Affairs
- Infrastructure and operations support by Modica

Current .govt.nz context

- Website and SRS interface are old



A little bit 1994.

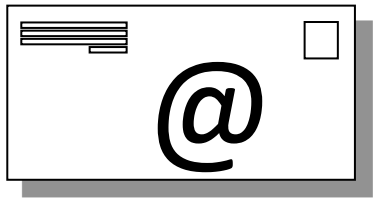
Current .govt.nz context

- Website and SRS interface are old
- Only ~30% of .govt.nz use our name servers
- Service lacks a number of features
  - Easy, self-serve DNS management
  - Built-in support for Māori names (i.e. macrons)
  - Name server redundancy (AKL & WGTN only)
  - Limited user authentication
  - DNSSEC

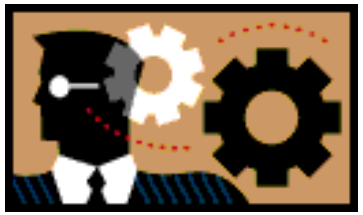
Current change process

Current process is very “manual”

Govt employee

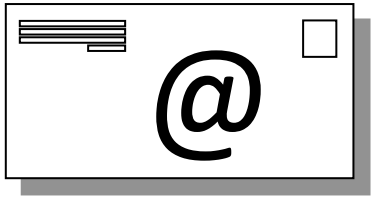


Emails DNS request to DIA

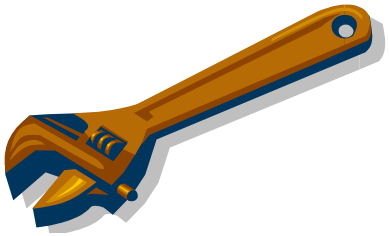


DIA verifies requester

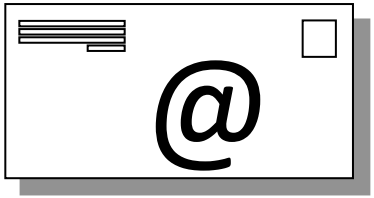
DIA forwards request to Modica



Modica actions request



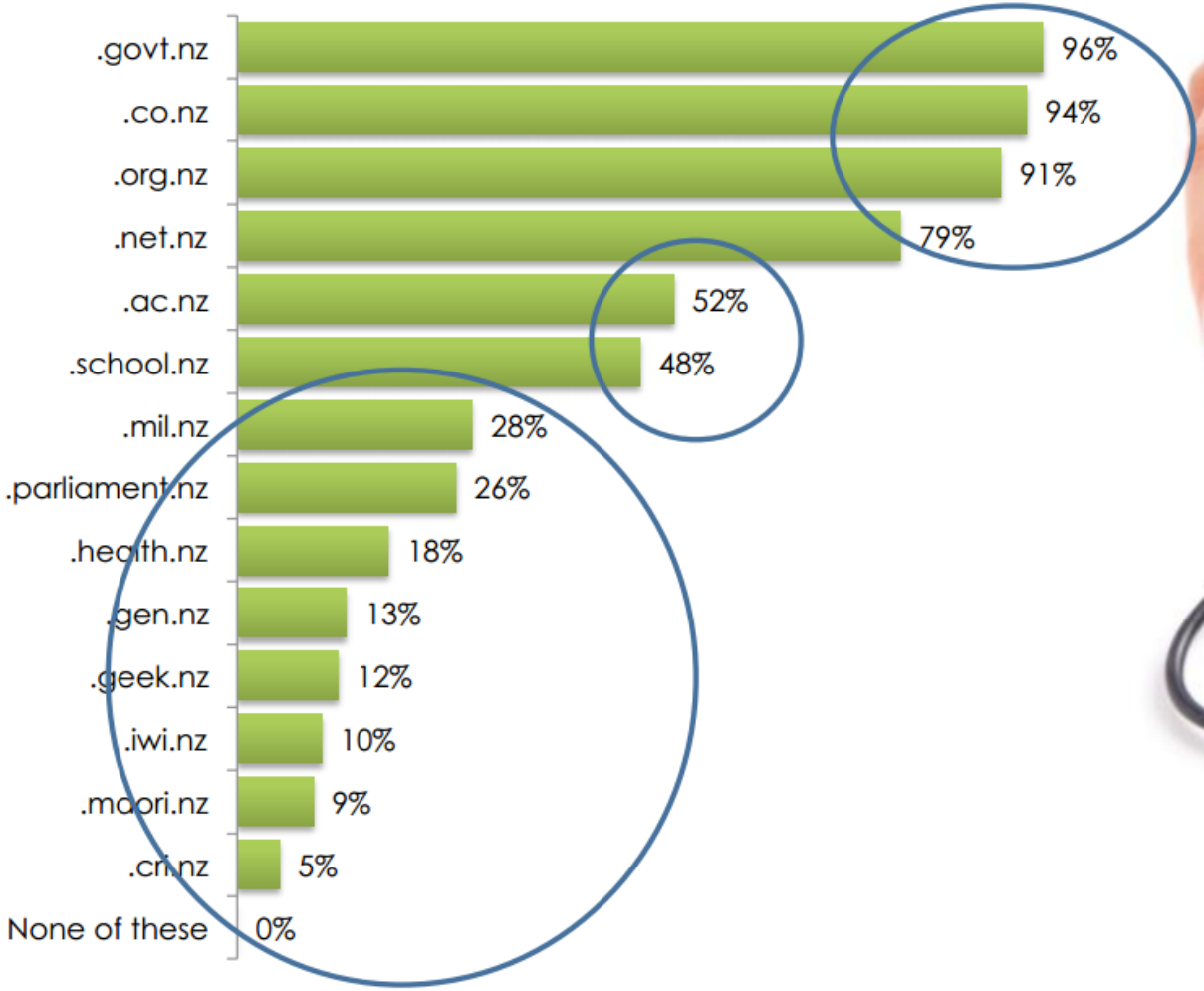
Modica emails requester and DIA



New .govt.nz context

- So we are rebuilding…with Modica's help
- New online DNS management portal
  - 24/7 easy, self-serve DNS management
  - Built-in support for Māori names (i.e. macrons)
  - Two-factor user authentication
  - Better name server redundancy (AKL, WGTN, & Sydney)
  - DNSSEC!
- But why DNSSEC?!?

Which second level domain names ending in .nz have you seen or heard of?



Base: Weighted results representative of New Zealand's online population (**n=1014**)

A '…critical factor for government sites are signs for credibility such as the domain ending ".gov" in the address bar…'

[Peters et al. (2011) Service delivery in one-stop government portals: observations based on a market research study in Queensland.]

Trust in .govt.nz

- .govt.nz is a strong brand
- NZ Government websites are implicitly trusted
- ".govt.nz" identifies a trusted, authentic resource
- We need to reinforce and enhance that trust

Online is becoming Government's primary channel

Better Public Services: Result 10

New Zealanders can complete their transactions with government easily in a digital environment

Key target:

- An average of 70 per cent of New Zealanders' most common transactions with government will be completed in a digital environment by 2017.

Reduced appetite for risk

Also,
there's the GC*B.

Wait!
That's too obvious.

Let's call them
the G*SB.

DNSSEC

==

Authenticity and integrity

==

Trust in .govt.nz

==

Protection from some misuse

Side benefits

Attract more agencies to our name servers

- Robustly configured
- Well-managed
- Seamless DNSSEC
- **All for free!**

Some implementation details

- DNSSEC key material stored in two locations: Wellington and Auckland
- True hardware security modules
- Only .govt.nz domains using our name servers get DNSSEC for free
- Totally seamless and invisible to agencies
- Automatic key rollovers
- Annual key generation ceremonies

Implementation timeline

- DNS service upgrade project began mid-2013
- Took time to gather requirements
- DNS operations deceptively simple
- DNSSEC doubly so!
- **Key Ceremony dress rehearsal:** 22 August
- **Actual Key Ceremony:** 23 October
- **New DNS service with DNSSEC:** March 2015

Key ceremony dress rehearsal

- 22 August 2014
- 12 people, including two witnesses from NZRS
- Managed to generate all the keys, but then ran into some hiccups -- that's what rehearsals are for

Key ceremony – the Real Deal

- 23 October 2014
- 13 people, including three witnesses, one from NZRS
- Completed all steps, with only a few minor events
- All-in-all a success: all keys generated and stored

Lessons Learned

- Leverage existing resources, e.g. NZRS DPS
- Talk to experts and those who have already done it, e.g. NZRS
- Find a BA with a strong aptitude for technology, technical minutiae, and detailed documentation

"Plan, plan, plan, plan, plan, plan, and plan."

Lessons Learned

- Script as much of every step as possible, including pre- and post- key ceremony activities
- Hold the key ceremony in a large room with two separate areas:
  - One area to serve as the action centre
  - One area for participants not doing anything – there can be lots of down time for some participants!

What went well

- Informed by our dress rehearsal, we had a very detailed key ceremony script: ~500 discrete steps
- It can seem tedious, but at step 273, you might ben tired or bored, but you know exactly what to do, what came before, and what comes after
- A detailed script also helps forecast how long the remaining steps will take

If we had to do it again…

- Consistent personnel throughout
- Comprehensive set of key ceremony contingency plans for when things don't go to script
- More rehearsals, at least for crucial roles

Next steps?

- Help agencies that are not using our name servers implement DNSSEC (which is really just a way to get them to come over to ours)
- Look into DANE and issuing our own certificates for government sites and services (pending better browser support)