2014 dns.govt.nz Project

modica

Authenticating .govt.nz via DNSSEC

Mark Goldfinch

Modica's Role

modica

- 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.

Project Deliverables

modica

- 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.

Design Considerations

modica

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

Design Considerations

modica

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

Design Considerations

modica

- 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**.

DNSSEC Automation

modica

- 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.

HSMs

modica

- 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.


TRADER JOE'S
I can see no way in which this carefully laid plan could ever fail.

DNSSEC Considerations

modica

- 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!**