.geek.nz Submission

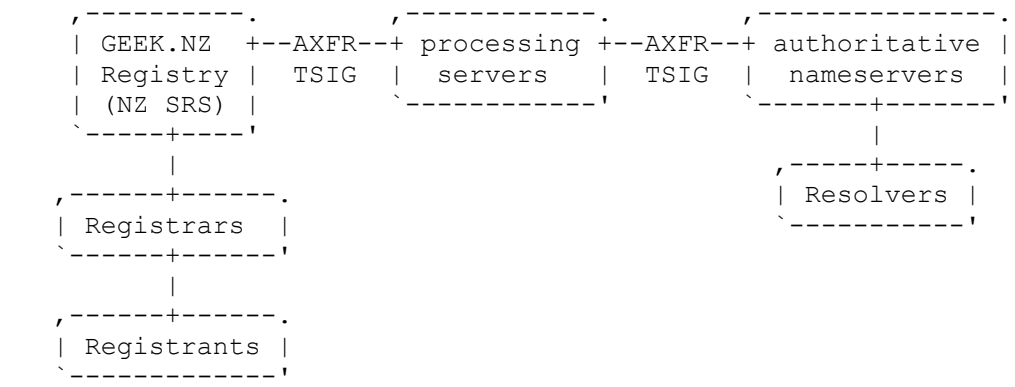
From: Joe Abley, Dean Pemberton, Andy Linton.
Received: 20 June 2003

Abstract

This submission proposes an implementation strategy for for the GEEK.NZ domain, should its creation be approved by InternetNZ. It is proposed to marry stability, affordability and widespread availability to registrants by way of the now-established NZ SRS with a framework within which new technology such as DNS security can be applied externally.

1. Overview

The general approach proposed in this document is to take advantage of the existing NZ SRS infrastructure to provide registry services for the GEEK.NZ domain, and to produce a set of authentic, known-good delegation data for publication in the DNS. This data will be securely transferred to one or more processing servers for signing [1]. The signed zone will then be securely distributed to a set of authoritative nameservers using standard protocols.



GEEK.NZ will represent a secure entrypoint into the DNS. Resolvers which are able to obtain a trusted copy of the public key used to sign the zone will be able to verify the authenticity of replies received from the GEEK.NZ servers.

The absense of a formal framework of zone signing with authority delegated from the root zone means that the practical value of the security provided by this proposal may not be substantial; however,

by experimentation in production zones in which accessible registry service is available we hope to gain valuable experience which will facilitate the future deployment of DNS security in other domains (within the NZ domain and elsewhere).

2. Benefits

1. Operational experience in integrating DNSSEC [1] as an extension to existing NZ SRS registry services. GEEK.NZ will function as a testbed, facilitating the roll-out of security extensions into other second-level domains promptly and with minimal risk as DNS security is rolled out into the production DNS root.

2. Operational experience with the interaction between resolvers and authoritative nameservers with signed zone data.

3. Providing a naturally early-adopting community of registrants with an opportunity to sign their own zones, and to manage a signed delegation [2] from the GEEK.NZ zone. Delegation signing and corresponding key management issues are an important aspect of the deployment of DNS security, and providing an accessible and visible test environment will provide valuable experience.

4. Nameserver independence. By arranging nameservice for GEEK.NZ on a different set of nameservers to the other NZ SRS-managed zones, any nameserver functionality required to support enhanced service (security extensions, IPv6 transport) can be provided with zero possible impact on the operation of other second-level domains under NZ.

3. Registration Services

Registration services for GEEK.NZ will be provided by the NZ SRS. Registrars will send transactions to the NZ SRS for names registered in the GEEK.NZ domain in the same way that they do for other second-level subdomains of NZ. GEEK.NZ registry transactions will be billed with an identical tariff to CO.NZ registry transactions.

4. Name Service

The NZ SRS will generate and publish a GEEK.NZ zone on one or more master nameservers. The zone will be retrieved using zone transfers [3] secured with TSIG [4] by one or more nominated processing servers.

The processed zone will be distributed to a set of authoritative nameservers, again using zone transfers secured with TSIG. This set of nameservers will include a diverse set of hosts within New Zealand, and other hosts distributed widely around the global Internet.

5. Infrastructure

Offers of slave nameservice from various professionally-operated nameservers in various countries including New Zealand, USA, Canada, Sweden and Amsterdam have already been received. Several of these nameservers are operated as high-performance clusters, and are already providing authoritative nameservice for substantial numbers of ccTLD zones. IPv6 nameservice from diverse locations will be available.

Professionally-adminstered facilities for processing the GEEK.NZ zone are available.

The GEEK.NZ public key (specifically, the public key used to sign the zone-signing key, also known as the "key signing key") will be distributed widely. Copies of the corresponding secret key will be stored securely in multiple locations.

6. Roles and Responsibilities

It is proposed that the NZ ccTLD manager should take full policy and operational control of the operation of the GEEK.NZ registry, but that responsibility for the operation of the GEEK.NZ zone be delegated to an external organisation. The terms of that delegation of responsibility should include provisions to ensure that the integrity of delegation data produced by the GEEK.NZ registry is preserved during the process of publishing the signed GEEK.NZ zone.

7. Implementation Details

A complete implementation plan based on this proposal will require numerous contractual and infrastructural details to be specified. It is not anticipated by the authors of this document that such specification will present substantial technical or administrative difficulties.

References

[1] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[2] Gudmundsson, O., "Delegation Signer Resource Record (work-in-progress)", I-D draft-ietf-dnsext-delegation-signer-15, June 2003.

[3] Gustafsson, A., "DNS Zone Transfer Protocol Clarifications (work-in-progress)", I-D draft-ietf-dnsext-axfr-clarify-05, November 2002.

[4] Vixie, P., Gudmundsson, O., Eastlake 3rd, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

Authors

Joe Abley
automagic.org

Dean Pemberton
FlatNet

Andy Linton
Lionra, New Zealand