Consultation on DNSSEC Implementation

.nz is preparing to introduce the Domain Name System Security Extensions (DNSSEC) to strengthen the security and reputation of .nz.

Vulnerabilities exist in the Domain Name System (DNS) that allow miscreants to re-direct, intercept, or modify users' Internet traffic, each with potentially devastating consequences. DNSSEC has been developed to add to the security features of the DNS, and to mitigate those vulnerabilities.

This document has been prepared as we seek to consult on the issues identified for Registrants and Registrars, and the proposed solutions. A background paper on DNSSEC can be accessed here.

DNS Management

Registrants can elect to operate their own DNS or they can delegate this responsibility to a third party called a 'DNS Operator', who offers DNS management services. The DNS Operator could be the Registrar for the domain, a Registrar who does not manage the domain, a hosting provider, an ISP, or some other third party that offers DNS management services.

Key Management

As noted in the background paper a core component of DNSSEC is the management of cryptographic keys. Registrants or DNS Operators need to store the public part of a cryptographic key in a DNS Resource Record, called a DNSKEY, in the zonefile for the domain. To enable the DNSKEY to be authenticated, a DS (Delegation Signer) Record needs to be generated and added to the Registry.

Currently only authorised .nz Registrars are permitted to add and update information that is held in the Registry.

It is proposed that:

- *Registrants or their DNS Operator will be responsible for generating and managing their keys.*
- *Registrants or their DNS Operator will be responsible for generating the DS Record.*
- *DS Records will be added to the Registry and maintained only via authorised .nz Registrars.*
- *The DS Record will be included in the WHOIS record for signed domain names, if applicable.*

One issue relating to key management is whether a DNS Operator generates one DNSKEY that is shared across multiple names, or whether they generate a key per name. While one shared key simplifies management, if that key is compromised then it affects multiple customers. The security of the private part of the cryptographic keys is critical to maintaining the integrity of those keys, and they should be protected accordingly.

- *It is proposed that DNS Operators set their own standards relating to DNSKEY management, and that these can be used as a point of difference from other DNS Operators.*

Another issue under key management relates to the updating of keys which is referred to as *rolling the keys*, or a *key rollover,* and how often this should be performed.

- *It is proposed that Registrants or their DNS Operator be responsible for determining how often they perform key rollovers.*

Transferring Signed Names

The transfer of a signed name needs to be managed properly to ensure that the transfer does not result in the domain being unreachable for a period of time due to resolution errors. Resolution errors can occur when DNSSEC-capable resolvers are unable to verify the information that has been sent to them.

Registrars by their very nature, through having a contract with DNCL, can be required to assist in ensuring that the transfer process is successful.

For Registrars it is proposed that:

- *Changes cannot be made to any details in the same transaction as a transfer, including changes to name servers.*

- *The following cooperation and participation will be required by Registrars, when involved in the transfer of a signed domain name, where the Registrant wants to modify DNSSEC related information:*
  - *The gaining Registrar must provide the new DNSKEY to the losing Registrar.*
  - *The losing Registrar must add the new DNSKEY to their DNS for the domain name and continue to serve this until they are notified that the change is complete.*
  - *The gaining Registrar provides the DS Record to the losing Registrar, who then provides it to the Registry.*
  - *Once the new DNSKEY and DS Record are visible to DNS resolvers then any changes to the name servers can be processed.*
  - *The name is then transferred.*
  - *The losing Registrar must remove the domain name from their system when requested, but must not remove it before being requested to do so.*
  - *The gaining Registrar can then delete the old DNSKEY provided by the losing Registrar.*

- *Where a forced bulk transfer is required, signed names will be transferred to a DNSSEC-Capable Registrar.*

Transferring to a Registrar that is not DNSSEC-capable

Registrars will be able to determine whether they become DNSSEC-capable or not. A signed name can be transferred in to a Registrar that is not DNSSEC-capable and resolution errors should not occur as long as there are no changes to the record. However if the Registrant wants to modify any DNSSEC related information, such as performing a key rollover, then they will need to transfer to a DNSSEC-capable Registrar.

- *It is proposed that Registrars who are not DNSSEC-capable be required to check if a*

name is signed before it is transferred in. If the name is signed then the Registrar will need to notify the Registrant of the implications of transferring in a signed name, and the Registrant will need to confirm the transfer, before the Registrar can initiate it.

DNS Operators who are not Registrars

If a Registrant has elected to delegate their key management to a DNS Operator, then the participation and cooperation of their DNS Operator will also be required. However as noted above, while DNCL does have contracts with Registrars, there are no contracts with DNS Operators. Registrants need to be aware that DNS Operators can not be held to account to the .nz policies, and cannot be required to participate and cooperate during transfers.

- *Question: How can the participation and cooperation of DNS Operators be encouraged?*

Un-signing a name

Once a name has been signed and the Registrant decides that they no longer require DNSSEC to protect the name, the name needs to be un-signed. Un-signing a name may result in the domain being unreachable for a period of time due to resolution errors.

- *It is proposed that when a Registrant elects to un-sign a signed name, the Registrar will be required to remove the DS Records as soon as practical to do so.*

As the .nz DNSSEC project progresses resources for Registrants and Registrars, such as a FAQ, will be added to the DNCL website.

Comments on the issues identified in this paper and the proposed solutions, should be sent by email to policies@dnc.org.nz, by fax to (04) 495 2115, or by mail to P O Box 11881, Wellington. As submissions are received they will be published on the DNC website here. Submissions should be received by midday on Monday 11 October 2010.