.nz NEWSLETTER – August 2010

:: Domain Name Commission ::

Expert and Mediator - .nz Dispute Resolution Service

The Domain Name Commission is responsible for managing the .nz domain name space (all domain names ending .nz) and administers a Dispute Resolution Service (DRS).

The DRS is a quick and cost-effective way of resolving domain name disputes and offers an accessible alternative to the courts. We are currently inviting applications for one Expert and one Mediator position.

Under the .nz DRS, mediation is the first tier of dispute resolution, and involves the mediator facilitating telephone (and email) mediation between parties to a domain name dispute within a set timeframe. If Mediation doesn't resolve the dispute, then the Complainant may refer the matter to an Expert for determination.

When an Expert is assigned to a case, he or she must evaluate and prepare a written decision within a set timeframe. The decision is binding on both parties to the dispute and will be published in full on the Domain Name Commission's website at **www.dnc.org.nz/decisions**.

Mediators and Experts are assigned by rotation to a case, and can expect to handle approximately four cases a year, with a fixed remuneration per case. In order to be considered for one of these positions, you will have a general knowledge of domain name and trade mark issues as well as proven ability in your field. Suitable candidates may be involved in the internet industry, mediation or arbitration, or legal profession, and will be a member of an appropriate professional organisation.

Further information on the DRS and these positions is available at **www.dnc.org.nz/information-experts** and **www.dnc.org.nz/information-mediators**. Candidates should familiarise themselves with this material before applying. Applications are invited by sending your CV and a covering letter. Successful candidates will be retained on a fixed term contract.

Please send your application to **vacancy@dnc.org.nz** no later than **2 September 2010**.

Consultation Paper on Registrant Search Functionality

Following a previous public consultation regarding additional search functionality for .nz domain names, it has been agreed by the DNCL Board that limited searches by registrant name should be permitted.

To allow such searches to be introduced, the current WHOIS policy needs to be reviewed. A marked-up copy of the current WHOIS Policy showing the proposed changes to incorporate a registrant search is available at
www.dnc.org.nz/content/Proposed_WHOIS_policy_amendments.pdf

Comments on the proposed changes to the WHOIS Policy, or on any aspect of the policy, 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 at http://dnc.org.nz/registrant-search-functionality . Submissions should be received by midday on **Monday 6 September 2010.**

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, un-signing that name may result in resolution errors, where resolvers cannot verify the authenticity of the information about the domain name. Resolution errors could result in that domain name being unreachable for a period of time via some resolvers.

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.

Statistics

In July, the number of active .nz domain names increased from 402,331 to 405,787, a net increase of 3,456.

Figures as at 31 July 2010:

	Active names as at 1 July	*Active names as at end 30 July*	*New registrations July*	*Renewals July*	*Net Growth*
.ac	1,771	1,793	46	329	22
.co	348,082	351,038	7,687	64,536	2,956
.cri	14	14	0	1	0
.geek	994	1,006	32	215	12
.gen	1,289	1,311	37	294	22
.govt	1,053	1,057	4	998	4

.health	111	115	4	3	4
.iwi	72	75	3	11	3
.maori	583	601	28	82	18
.mil	26	26	0	4	0
.net	22,312	22,492	505	4,413	180
.org	23,017	23,245	490	4,409	228
.parliament	7	7	0	7	0
.school	3,000	3,007	21	1,249	7
TOTAL	402,331	405,787	8,857	76,551	3,456

Note: these figures do not include names in the 'pending release' status. They incorporate all active domain names in the .nz register. For more statistics, see http://dnc.org.nz/statistics

:: .nz Registry Services ::

Availability

Availability %	SLA	May	June	July
SRS	99.90	100	100	100
Whois	99.90	100	100	100
DNS	100	100	100	100

SRS Response times

Performance figures on the production environment for the previous three months:

Avg Response time (in seconds)	SLA Target	May	June	July
Domain Details Query	≤0.5	0.03	0.03	0.02
Domain Update	≤0.8	0.19	0.23	0
Domain Create	≤0.8	0.25	0.25	0
Get Message	≤0.5	0.03	0.03	0.04
Whois	≤0.5	0.09	0.08	0.09
Whois queries at back end including Registrar (volume 000's)	N/A	3,718	3,833	3,645
Whois Server Queries (volume 000's)	N/A	713	737	851
UDAI Valid Query	≤0.5	0.11	0.08	0.11

Server DNS % Availability

	May	June	July
NS1	100	100	100
NS2	100	100	100
NS3	100	100	100
NS4	100	100	100
NS5	100	100	100
NS6	100	100	100
NS7	100	100	100

Unscheduled Outages during July 2010

Outage Type	Total Duration
SRS Unscheduled	
WHOIS Unscheduled	
DNS	

Scheduled Outages during July 2010

Outage Type	Total Duration
SRS Scheduled	4 hours
SRS Emergency Scheduled	
Whois Scheduled	4 hours
Whois Emergency Scheduled	

Planned Scheduled Outages

Details of future SRS releases and planned scheduled outages can be found on our website.http://www.nzrs.net.nz/notices/updates.shtml

Disaster Recovery Handover Test

On Sunday, 5th September 2010 there will be a scheduled shut down of the SRS to allow for the yearly Disaster Recovery Handover Test. The test will be based on the Backup Operation Support Service (BOSS) activation handover procedure. The object of the exercise is to test as much of the SRS disaster recovery procedures as possible in a controlled and safe manner.

The test will occur on Sunday 5th September (4 hours) 06:00 - 10:00 NZST.

EPP

The final version of the SRS EPP interface will be deployed to our test environment on the 30th August and we are targetting the date of the 12th of September for deploying the EPP interface

into production. If there are any registrars that would like to assist us with our testing or are interested in using the EPP interface in production then please contact Dave or Manu on support@nzrs.net.nz.

DNSSEC

We are actively working on the DNSSEC deployment for .nz. We have chosen a signing architecture based on OpenDNSSEC and the Sun Crypto Accelerator 6000 for the Hardware Security Module. Currently we are making changes to the SRS system to support DS records and testing the signing architecture. We expect to have the .nz zone signed by the end of the year, the second level zones will follow in a reasonable timeframe. If you have any questions, please don't hesitate in contacting us at support@nzrs.net.nz

Any Comments?

If you have any questions or concerns about the SRS, please don't hesitate to contact us. For registry or technical matters, contact Dave Baker at support@nzrs.net.nz or on 04 931 6970. For all other matters, contact Debbie Monahan at info@dnc.org.nz.

Please Note

If you would like to be notified of future updates, please use the SUBSCRIBE function on the DNC site and select the category 'Newsletters'. If you ever want to stop receiving our newsletter, please send an email with 'Unsubscribe' in the subject line to unsubscribe@dnc.org.nz