DNS Security FAQ for Registrants

DNSSEC has been developed to provide authentication and integrity to the Domain Name System (DNS). The introduction of DNSSEC to .nz will improve the security posture of New Zealand by providing Registrants with an effective tool to combat attacks such as website phishing.

The following FAQ has been prepared to provide an introduction to Domain Name System (DNS) Security.

DNSSEC Overview

- What is the DNS?
- What is DNSSEC?
- Do I need to enable DNSSEC on my domain name?
- What are the benefits of DNSSEC?
- What does DNSSEC NOT address?
- Do I need DNSSEC if I have SSL?

Threats to the DNS

- What are the threats to the DNS?
- What is DNS Spoofing?
- What are Malicious Resolvers?
- What is a Man in the Middle (MITM) Attack?
- Example scenario of the threats

Setting up DNSSEC

- How can I setup DNSSEC for my .nz domain name?
- Where can I find .nz Authorised Registrars who offer DNSSEC?
- What does "DNSSEC Friendly" mean?
- What does "Handles DS Records" mean?

How DNSSEC works

- How does DNSSEC work?
- What is the 'Chain of Trust'?
- What is involved with the management of DNS and DNSSEC Keys?
- What is a DNS Operator?
- What is Key?
- What is a Key Rollover?

DNSSEC Overview

What is the DNS?

The Domain Name System (DNS) is like the white pages for the Internet – mapping the Internet Protocol (IP) addresses to domain names that are easy to read.

For example the domain name for this website is www.dnc.org.nz, and the website is located on a computer server that has the IP address 202.78.240.52. It is the DNS that translates that domain name into the IP address, so that your browser can find the location of the server to request the website you want to view.

The DNS was designed early in the history of the Internet and was not designed with security in mind. Vulnerabilities exist in the DNS that can be exploited allowing attackers to intercept, re-direct, or modify your Internet traffic.

DNSSEC was developed in response to these vulnerabilities.

What is DNSSEC?

The Domain Name System Security Extensions (DNSSEC) have been developed to improve the security of the Domain Name System (DNS) and provide increased protection for activities such as browsing the Internet and email. DNSSEC is in the process of being rolled out internationally.

DNSSEC ensures that the website displayed on your computer really is the genuine website that you intended to visit. It works, in simple terms, by using encoded "keys", similar to passwords, that your web browser looks up in the DNS to verify that you are viewing the genuine website.

The Internet's root zone was signed earlier this year, and increasing numbers of Country Code Top Level Domains (ccTLDs) and Generic Top Level Domains (gTLDs) are now being signed.

.nz, a ccTLD, has deployed DNSSEC, and all of the second level domains such as .co.nz, .govt.nz and .org.nz will be signed in 2012. The deployment schedule can be found here: http://nzrs.net.nz/dns/dnssec

Registrants must now decide whether they wish to deploy DNSSEC for their domain names at the third level to provide these assurances to visitors to their site e.g. In the domain name **dnc**.org.nz, "dnc" is at the third level.

Do I need to enable DNSSEC on my domain name?

While every website could benefit from implementing DNSSEC the priority should be for those websites that are concerned about the integrity of their domain name, such as those that process financial and personally identifiable information, and sites that are at a higher risk for malicious activity.

What are the benefits of DNSSEC?

DNSSEC has been developed to provide authentication and integrity to the DNS to mitigate threats (listed below) , while ensuring that backwards compatibility is maintained.

- *Origin Authentication and Data Integrity*
  DNSSEC-capable resolvers are able to digitally verify that the DNS data they receive is identical to the information on the authoritative DNSSEC-capable name server. This is done by authenticating the origin and integrity of DNS data as it transits the Internet.

- *Authenticated denial of existence*
  DNSSEC-capable resolvers are able to determine whether or not a resource, such as a name server, actually exists.

One example of the benefits that DNSSEC provides is that owners of websites and email servers that have implemented DNSSEC, will have a higher degree of certainty that visitors to their website and emails destined for their email servers, will not be redirected elsewhere.

What does DNSSEC NOT address?

DNSSEC does not provide confidentiality for data that is transmitted.

Do I need DNSSEC if I have SSL?

The short answer is yes, as DNSSEC and SSL provide different types of protection. SSL aims to provide data confidentiality by encrypting the connection between websites and the web browsers of its visitors. DNSSEC provides Origin Authentication of DNS data, Data Integrity, and Authenticated Denial of Existence.

Threats to the DNS

What are the threats to the DNS?

Vulnerabilities in the DNS are being actively exploited by attackers. These attacks are often undetectable to users. The attacks, which DNSSEC addresses, can be categorised into the following:

- *DNS Spoofing* (malicious cache poisoning)
- *Malicious Resolvers*
- *Man in the Middle (MITM) Attacks*

What is DNS Spoofing?

This is where a DNS name server is manipulated into accepting and storing false data that is not from a trusted DNS source, and reissues that false data.

One way this is used by attackers is to modify the IP address for a website, so that visitors to that website are unknowingly redirected to a fraudulent destination selected by the attacker. For example, criminals may redirect users to a fake banking website. They can then harvest all of the usernames and passwords entered on the fake website, and use them on the legitimate website to withdraw funds.

What are Malicious Resolvers?

A resolver is the client-side or local part of the DNS, and initiate DNS queries to lookup the IP address of a given resource, such as website. As the DNS is a hierarchical system many DNS Servers can be involved in the lookup and DNS servers in the chain can also act as resolvers as they pass along the lookup request.

Malicious resolvers provide fraudulent DNS responses in an attempt to redirect your Internet traffic to a fraudulent destination or website.

What is a Man in the Middle (MITM) Attack?

This is where an attacker is able to redirect, intercept, and modify network traffic. Because DNS does not provide any data integrity checks an attacker can intercept, and modify, legitimate DNS requests or responses. This can also result in an attacker redirecting you to a fraudulent destination of their choosing.

Even a single compromised DNS name server can have a large scale impact because one DNS server can serve many thousands of DNS requests.

Example scenario of the threats

The following scenario has been prepared to illustrate how vulnerabilities in the DNS are being exploited by miscreants and how DNSSEC mitigates those threats.

The goal of the attacker is to redirect the customers of a banking website to a fraudulent website, under the attacker's control, to harvest customer's credentials. In the following scenario neither the target bank nor ISP have implemented DNSSEC.

- The attacker sets up a fake banking website that looks identical to a legitimate bank's website.
- The attacker then inserts fraudulent data into an ISP's DNS servers, with the IP address for their fake website.
- When any customers of the targeted ISP enter the website address for the targeted bank into their browser, the ISP's DNS server provides the customer with the fraudulent IP address, redirecting their customers to the attacker's website.
- When the customers log into the fraudulent website their usernames and passwords are captured and recorded by the attacker.
- The attacker then uses those credentials to log into the targeted bank's website, masquerading as a legitimate user, and transfers funds to an account they control.

In this scenario if either the bank or the ISP had implemented DNSSEC then the ISP's customers may not have ended up being redirected to the attacker's fraudulent website.

- If the bank had implemented DNSSEC, the customer's computer may have detected the fraudulent IP address when it attempted to validate the response from the ISP's DNS server.

- If the ISP had implemented DNSSEC then the ISP's caching server would have rejected the attempt to poison its cache.

Two real world examples similar to the example above can be found here:

- Brazilian Bank Bandesco
- Irish ISP Eircom

Setting up DNSSEC

How can I setup DNSSEC for my .nz domain name?

When you deploy DNSSEC on a domain name it is referred to as “signing” the domain name. You can contact your .nz Registrar to see if they offer DNSSEC services, or you could contact a third party DNS Operator who may offer DNSSEC services. You should be aware that the Domain Name Commission does not have any formal relationships with DNS Operators who are not .nz Authorised Registrars. Therefore the DNC cannot mandate their cooperation and participation in the management of DNSSEC signed domain names.

Where can I find .nz Authorised Registrars who offer DNSSEC?

The Domain Name Commission's website has a list of all Authorised .nz Registrars at www.dnc.org.nz/registrars. The list shows which registrars offer DNSSEC and which are 'DNSSEC Friendly'.

What does "DNSSEC Friendly" mean?

This status identifies Registrar’s that meet a higher level of service relative to offering DNSSEC services in the .nz space. The Domain Name Commission recommends that Registrants looking to deploy DNSSEC look for Registrars who are DNSSEC Friendly.

What does “Handles DS Records” mean?

This status identifies those Registrars who have the capability to update the SRS with DS Records.

How does DNSSEC work?

How does DNSSEC work?

DNSSEC uses public key cryptography to digitally sign DNS data. DNSSEC-capable resolvers are able to verify whether the data contained in a DNS response comes from an authoritative DNS server and whether it has been altered.

What is the ‘Chain of Trust’?

DNSSEC works in a chain, and each part of the chain must be signed for the whole signature to be valid. DNS Resolvers need to be able to fetch the public key and verify that it can be trusted.

The public key to validate a domain name’s data can be obtained from the domain name’s authoritative servers. To establish the trust on a key, you can get a copy through an offline trusted channel or use a ‘Chain of Trust’.

A ‘Link of Trust’ is established between a child zone and its parent. The child zone provides a digest of the keys, known as a Delegation Signer (DS) Record, to the parent and the parent validates and signs it, using its own key. The step is repeated up the hierarchy creating a ‘Chain of Trust’ that can be followed.

For example the Chain of Trust for dnc.org.nz is established through the keys for dnc.org.nz being signed by the .org.nz zone keys. The keys for the .org.nz zone are signed by the .nz zone keys and the keys for the .nz zone are signed by the keys for the root '.' (dot) zone. This forms the Chain of Trust that can be ‘walked’ from the DNS root zone down to dnc.org.nz.

What is involved with the management of DNS and DNSSEC Keys?

As DNSSEC uses public key cryptography, the existence and management of a cryptographic key for each domain name that implements DNSSEC is required.

Registrants can elect to operate their own DNS or they can delegate this responsibility to a third party called a ‘DNS Operator’.

At some point after DNSSEC has been implemented on a domain name, and it’s DNS records have been signed, changes to the DNS data may be needed. The changes may be DNSSEC related, such as updating the key used to sign the data, or transferring a domain name registration to another Registrar.

These changes will need to be properly managed and additional steps are required to ensure that resolution errors do not occur. Resolution errors may result in DNSSEC-capable resolvers being unable to verify the information that has been sent to them, and this may result a domain being unreachable for a period of time.

What is a DNS Operator?

A DNS Operator could be the Registrar for your domain, a Registrar who does not manage your domain, a hosting provider, an ISP, or some other third party that offers DNS management services.

What is a Key?

DNSSEC uses cryptographic ‘keys’ to to verify whether the data contained in a DNS response comes from an authoritative DNS server and whether it has been altered.

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 .nz Registry. Only DNSSEC capable Registrars can add this information to the Registry.

Registrars who are able to handle and process DNSKEYs and DS Records are listed on the .nz Authorised Registrars list at: http://dnc.org.nz/story/authorised-registrars

What is a Key Rollover?

The updating of DNSSEC keys is referred to as *rolling the keys*, or a *key rollover.*