DNSSEC Practice Statement

- 1. Introduction
  - 1.1. Document Name and Identification
  - 1.2. Community
  - 1.3. Applicability
  - 1.4. Document Management
- 2. Publication and Repositories
  - 2.1. Official publication site
  - 2.2. Publication of key signing keys
- 3. Operational Requirements
  - 3.1. Activation of DNSSEC for child zone
  - 3.2. Identification and authentication of registrant
  - 3.3. Registration of delegation signer (DS) records
  - 3.4. Method to prove possession of private key
  - 3.5. Removal of DS record
- 4. Management, Operational and Physical Controls
  - 4.1. Site Controls
  - 4.2. Key Material Controls
  - 4.3. Procedural Controls
    - 4.3.1. Trusted roles
    - 4.3.2. Other roles
    - 4.3.3. Number of persons required per task
    - 4.3.4. Trusted individuals
  - 4.4. Personnel Controls
    - 4.4.1. Qualifications, experience, and clearance requirements
    - 4.4.2. Background check procedures
    - 4.4.3. Training requirements
    - 4.4.4. Contracting personnel requirements
    - 4.4.5. Documentation supplied to personnel
  - 4.5. Audit Logging Procedures
    - 4.5.1. Types of events recorded
    - 4.5.2. Frequency of processing log
    - 4.5.3. Retention period for audit log information
    - 4.5.4. Protection of audit log
    - 4.5.5. Vulnerability assessments
  - 4.6. Compromise and Disaster Recovery
    - 4.6.1. Incident Detection and compromise handling procedures
    - 4.6.2. Corrupted computing resources, software, or information
    - 4.6.3. Procedures in the event of suspicion of a compromised or incorrectly used private key.
    - 4.6.4. Business Continuity and IT Disaster Recovery Capabilities
  - 4.7. Entity Termination
- 5. Technical Security Controls
  - 5.1. Key Pair Generation and Installation
    - 5.1.1. Key pair generation
    - 5.1.2. Public key distribution
    - 5.1.3. Public key parameters generation and quality checking
    - 5.1.4. Key usage purposes
  - 5.2. Private key protection and Cryptographic Module Engineering Controls
    - 5.2.1. Cryptographic module standards and controls
    - 5.2.2. Private key (m-of-n) multi-person control
    - 5.2.3. Private key escrow
    - 5.2.4. Private key backup
    - 5.2.5. Private key storage on cryptographic module
    - 5.2.6. Private key archival
    - 5.2.7. Private key transfer into or from a cryptographic module
    - 5.2.8. Method of destroying private key
  - 5.3. Other Aspects of Key Pair Management
    - 5.3.1. Public key archival
    - 5.3.2. Key usage periods
  - 5.4. Activation data
    - 5.4.1. Other aspects of activation data
  - 5.5. Computer Security Controls
  - 5.6. Network Security Controls
  - 5.7. Time stamping
  - 5.8. Life Cycle Technical Controls
    - 5.8.1. System development controls
    - 5.8.2. Security management controls
- 6. Zone Signing
  - 6.1. Key lengths and algorithms
  - 6.2. Authenticated denial of existence
  - 6.3. Signature format
  - 6.4. Zone signing key roll-over
  - 6.5. Key signing key roll-over

- 6.6. Signature life-time and resigning frequency
- 6.7. Verification of zone signing key set
- 6.8. Verification of resource records
- 6.9. Resource records time-to-live

7. Compliance Audit
- 7.1. Frequency of entity compliance audit
- 7.2. Identity/qualifications of auditor
- 7.3. Auditor's relationship to audited party
- 7.4. Audit scope
- 7.5. Actions taken as a result of deficiency
- 7.6. Communication of results

1. Introduction

This document is the NZRS DNSSEC Practice Statement (DPS). It defines the operational procedures for the management of DNS Security Extensions (DNSSEC) in the New Zealand top-level domain (.nz) and second level domains under .nz.

This document draws on the Internet Engineering Task Force (IETF) I-D for DNSSEC Practices Statement construction, but has a number of significant differences to keep the .nz DPS appropriate for .nz.

1.1. Document Name and Identification

Document title: DNSSEC Practice Statement

Version: 1.3

Last Update: Jul 17, 2017 10:58

1.2. Community

The following roles and delegation of liability with regard to DNSSEC have been identified:

- **Registry** NZRS is the registry, managing and operating the domain name register under .nz name space.
- **Zone Administrator** NZRS is the zone administrator and so responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys. NZRS is responsible for the secure export and publication of trust anchors (TA) and the registration and maintenance of DS resource records in the root zone.
- **.nz Zone Operator** NZRS is a .nz Zone Operator and from time to time employs external organisations as additional .nz Zone Operators. The .nz Zone Operators are not involved in any policy making or data modification.
- **Registrar** Registrars are responsible for securely identifying the Registrant of a domain, among other responsibilities detailed in .nz Registrar Roles and Responsibilities. Registrars are responsible for adding, removing and changing the DS records for each domain by Registrant request.
- **Moderator** Moderators are responsible for the membership of domains under a moderated 2LD. A moderated 2LD means that registrants need to meet specific additional criteria to register a domain, among other responsibilities detailed in the moderation policies.
- **Registrant** Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the Registrar. Registrants are responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost. Registrants may choose to delegate this responsibility to a registrar or third party zone operator.
- **Relying Party** The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate TAs. The relying part must also stay informed of an relevant DNSSEC-related events in the .nz domain.

1.3. Applicability

Each Registrant is responsible for determining the relevant level of security for their domain. This DPS is exclusively applicable to the top-level .nz and second level domains and describes the procedures and security controls applicable when managing and employing keys and signatures for the signing of the .nz zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the .nz domain and assess their own risk.

1.4. Document Management

NZRS is responsible for keeping this document updated. For updated contact details, please refer to http://www.nzrs.net.nz/contact.

This DPS is a living document and it will be updated when necessary, such as in the event of system or procedure modifications affecting the contents of this document.

Updates to this DPS will be made in the form of the publication of a new version of this document. Previous versions and changes will be made available with this document. This DPS and amendments to it are published at the site detailed in Section 2.1.

All new versions will be published at the site detailed in Section 2.1. Major revisions will also be announced to Registrars, NZNOG and any other groups that express an interest in receiving such notifications.

Only the most recent version of this DPS is applicable.

2. Publication and Repositories

2.1. Official publication site

NZRS publishes DNSSEC-relevant information on NZRS's website at http://www.nzrs.net.nz/dns/dnssec.

Notifications relevant to DNSSEC in .NZ will be distributed by e-mail through community-accepted forum.

2.2. Publication of key signing keys

NZRS will publish the .nz KSK in the form of DS records directly in the root zone when available. No other trust anchors or repositories are used.

3. Operational Requirements

3.1. Activation of DNSSEC for child zone

DNSSEC for a child zone is activated by publishing a signed DS record for that zone. Activation of DNSSEC must be explicitly requested by the registrant by submitting the DS records.

3.2. Identification and authentication of registrant

It is the responsibility of the Registrar to securely identify and authenticate the registrant through a suitable method for the task, and in compliance with their existing obligations in the agreement between .NZ and the Registrar.

3.3. Registration of delegation signer (DS) records

NZRS accepts DS records through the SRS/EPP interface from each Registrar. The DS record must be valid and sent in the format indicated in the SRS protocol specification if using the SRS or according to RFC 5910 if using EPP. Up to 10 DS records can be registered per domain name.

3.4. Method to prove possession of private key

NZRS does not validate if the Registrant is the holder of the private key. The Registrar is responsible for conducting the appropriate controls required and those considered necessary.

3.5. Removal of DS record

Only the Registrant has the authority to request the removal of the DS records.

A DS record is removed by Registrars sending a SRS/EPP request to the SRS to remove the DS record. The removal of all DS records for a domain name will cancel the DNSSEC security mechanism for the zone in question.

The Registrant tasks the Registrar with implementing the removal. The Registrar may only do this on behalf of the Registrant. Upon receipt of the removal request by the SRS, it takes no longer than until the next zone generation for the change to be recorded in the zone file. Hence, it takes up to two times the TTL plus the distribution time before the changes have been deployed. The whole procedure may take a maximum of five hours to complete.

There is no process to support faster removal of DS records in an emergency.

4. Management, Operational and Physical Controls

4.1. Site Controls

NZRS maintains two fully operational sites in New Zealand, located in Auckland and Wellington. Both contain a complete set of NZRS's critical systems, with updated information that's replicated automatically during normal operation.

The site located in Auckland is a purpose built state-of-the-art data centre and has the following security features:

- Swipe card and PIN are required for access
- Surrounding the facility is a perimeter fence with automatic gate
- On-site security staff are present 24-hours by 7 days a week
- Access is restricted to authorised personnel only and photographs and electronic logs are recorded for all access visits
- Upon entry to the building there are multiple key access doors to go through before entry into the server room
- The NZRS rack is located in a Co-Lo server room. The rack is locked at all times, access is logged and the room is monitored at all times by a control room operator via CCTV
- Authorised personnel and 3rd party's (eg hardware support engineers) have un-escorted access to the racks in the Co-Lo server room. 3rd party's must have prior approval given by an authorised person before entry is allowed.
- Electronic surveillance is used throughout the facility
  The site located in Wellington is in a data centre operated by a large national infrastructure services company. It is not located at the NZRS office. The server room has the following security features:
- Swipe card and PIN access
- Monitored security alarm
- Upon entry to the building there are multiple key access doors to go through before entry into the server room
- Access is restricted to authorised personnel only
- The NZRS rack is located in a Co-Lo server room. The rack is locked at all times, access is logged and the room is monitored at all times by a control room operator via CCTV.
- Authorised personnel and 3rd party's (eg hardware support engineers) have un-escorted access to the racks in the Co-Lo server room. 3rd party's must have prior approval given by an authorised person before entry is allowed.
- Electronic surveillance is used throughout the facility

In addition to the above:

- All facilities have power backed up by UPS and auto-start generators. The computer rooms in the facilities have air conditioning providing controlled temperature and humidity.
- All sites are equipped with fire alarm systems with smoke detectors positioned throughout the buildings. Fire suppression units are situated in the servers' rooms.
- All the facilities are located in areas not associated with a high risk of flooding and are situated well above the sea level.

4.2. Key Material Controls

Security of key material at these sites is ensured by the following means:

- DNSSEC key material is stored in a FIPS 140-2 Level 3 compliant HSM.

- All key related operations require the use of the HSM.

- Access to the private component of the keys is only possible as part of a backup. Exporting of keys in plain text is not possible.

- Media and other materials containing sensitive information is destroyed in a secure manner, by shredding in the case of documents or rendering unreadable in the case of media.

- Backups of key material are stored encrypted on removable media, stored inside a safe in a secure location in tamper evident bags, which are sealed during the Key Generation procedure. Integrity of backups is verified by checking the backup files' cryptographic hash previous to every Key Generation procedure.

- Backup and restoration of key material can only be initiated with the presence of two Keystore Security Officers and one System Administrator. Access to the backup media is restricted to NZRS's personnel in trusted roles only as specified in Section 4.3.1. The backup storage facility is administratively separated from NZRS facilities.

- A stolen key cannot be accessed, restored or used without the presence of two Keystore Security Officers and an HSM.

4.3. Procedural Controls

4.3.1. Trusted roles

Persons that are able to affect the zone file’s content, delivery of trust anchors or the generation or use of private keys, hold the following trusted roles:

- **System Administrator, SA**
  - Allowed to physically access the device containing the keys
  - Allowed full administration rights to the signing servers
  - Does not have access to the activation material of the HSM
  - Does not have access to the keys

    - The minimum number of SA's appointed will be 2 and the maximum will be 6

- **Keystore Security Officer, KSO**
    - Holds the credentials to access the keystore holding the keys
    - Does not have physical or logical access to the operational facilities
    - The minimum number of KSO's appointed will be 2 and the maximum will be 5

- **Device Security Officer, DSO**
    - Required to initialize the HSM and recover after a disaster
    - Does not have access to the keys
    - May have physical access or logical access to the operational facilities
    - The minimum number of DSO's appointed will be 2 and the maximum will be 5

The following trusted role is held by persons that are allowed to be present for the generation of private keys:

- **Key Generation Administrator, KGA**
    - Verifies the Key Generation procedure is executed according to the script and produces the execution log
    - Does not have access to the keys
    - Does not have physical access or logical access to the operational facilities
    - There is one KGA

All individuals who hold a trusted role are required to sign a confidentiality agreement and an agreement to acknowledge their responsibilities with NZRS. Before a person receives their credentials for system access, a valid form of identification must be presented.

The separation of duties is enforced by the access rules for each role. A Systems Administrator is not allowed to be a Key Security Officer and vice versa.

4.3.2. Other roles

- **Witness, WI**
    - May be present
    - Does not have access to the keys
    - Does not have physical access or logical access to the operational facilities

All witnesses are required to present a valid form of photo identification.

4.3.3. Number of persons required per task

- **HSM initialization and activation requires**
    - All Keystore Security Officers,
    - All Device Security Officers, and
    - One System Administrator

- **Key generation requires:**
    - One System Administrator and
    - Two Keystore Security Officers

- **Export of keys for backup purposes requires:**
    - One System Administrator and
    - Two Keystore Security Officers

For the above tasks the Witness will be invited to attend.

- **Key restoration from backup requires:**
    - One System Administrator and
    - Two Keystore Security Officers

None of the operations previously described may be carried out in the presence of unauthorized people.
For an emergency HSM initialization and activation the minimum presence of two Keystore Security Officers and one System Administrator is required.

4.3.4. Trusted individuals

All individuals with a KSO or KGA trusted role are permanent employees or directors of NZRS and have been subject to the background checks specified in Section 4.4.2.

All individuals with a SA or DSO trusted role are permanent employees of NZRS and have been subject to the background checks specified in Section 4.4.2.

4.4. Personnel Controls

4.4.1. Qualifications, experience, and clearance requirements

NZRS requires that personnel seeking to become Trusted Individuals present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities adequately.

4.4.2. Background check procedures

For the trusted roles in Section 4.3.1, the following background checks are included:

- Candidate resume
- Previous employments
- Reference check
- Credit check
- Criminal convictions check

Using this information, the NZRS CE would then decide on a case by case basis if the individual considered for a trusted role is suitable or not.

Outsourced partners, contractors and sub-contractors performing work on the NZRS account are required to:

- Undertake pre-employment checks for new employees
- Provide a list of all key personnel that perform work on NZRS systems and obtain NZRS approval
- Obtain prior approval from NZRS for any replacement of key personnel that work on NZRS systems
- Ensure all personnel that work on NZRS systems sign a NZRS confidentiality and non disclosure agreement

4.4.3. Training requirements

Every person with a trusted role in the Key Generation procedure must be trained in the Key Generation procedure and have taken part in the procedure training.

4.4.4. Contracting personnel requirements

NZRS takes all care to ensure that no person outside the Trusted Roles specified in Section 4.3.1 can get access to the signer or signing material such as backups.

4.4.5. Documentation supplied to personnel

NZRS supplies the necessary documentation to each employee to perform their work task in a secure and satisfactory manner.

4.5. Audit Logging Procedures

Logging is automatically carried out and involves the continuous collection of information regarding the activities that take place in an IT system. This logged information is used in the monitoring of operations, for statistical purposes and for investigation purposes in suspected cases of violation of .nz's policies and regulations.

Logging information also includes the journals, checklists and other paper documents that are vital to security and that are required for auditing.

4.5.1. Types of events recorded

The following events are included in logging:

- All Key Generation Procedures will be logged in electronic and handwritten logbook and copies will be stored in a safe location.
- All types of activities involving HSM, such as key generation and activation, key removal, exporting and restoration.
- Successful and unsuccessful remote access attempts
- The processing of security-sensitive information
- Entry to a facility

4.5.2. Frequency of processing log

Logs are systematically analyzed through automated and manual processes. Regular controls are applied, specifically around key generation, login attempts and detected anomalies.

4.5.3. Retention period for audit log information

Log information is stored in log servers for 4 months. Afterwards, the log information is archived for at least 2 years.

4.5.4. Protection of audit log

Log files are backed up into tape, and later transferred to a secure location. Paper logs are protected by copying and storing them in a secure fire-proof location.

4.5.5. Vulnerability assessments

Daily internal and external scans are performed using a third party vulnerability assessment tool.

In addition to the daily checks mention above on the logs, every two months the events registered in the logs are processed and analyzed to monitor for potential system vulnerabilities.

4.6. Compromise and Disaster Recovery

4.6.1. Incident Detection and compromise handling procedures

For the purpose of this document an incident is any event that caused or could have caused an outage, disruption, information corruption or security breaches.

All incidents are handled in accordance with NZRS's Security Incident Detection and Response Manual. This document indicates the cause of the incident has to be investigated, identify the effects, measures to prevent the recurrence of the event and channels and mechanism to report this information.

The NZRS core systems are designed with a multi-layer approach to security. NZRS use a number of specific incident prevention methods:

- System intrusion prevention and detection system using file verification software
- Universal "Security Information Event Management" (SIEM) system

NZRS have also implemented a range of general security practices that will help ensure that appropriate measures are taken to maintain business continuity, prevent, minimize the risk, and minimize the impact of security breaches.
Some of the security measures implemented by NZRS include:

- Business Continuity Plan
- Annual Audits and regular reviews
- Disaster Recovery Plan
- Backup Operations Systems Support and Activation Plans
- Patch Management
- Risk Management
- Security Policy
- Security Procedures
- Firewalls, secure configurations, passwords etc
- Monitoring of Security Advisories
- Scan external hosts for vulnerabilities
- Server hardening - disable services that are not required etc
- Comparison and reporting of changes/differences to configuration files
- Quality Assurance procedures

4.6.2. Corrupted computing resources, software, or information

In the event of corruption, the procedures detailed in the Business Continuity Management Manual shall be followed.

4.6.3. Procedures in the event of suspicion of a compromised or incorrectly used private key.

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:

- If a ZSK is suspected of having been compromised, it will immediately be removed from production and stopped being used. If necessary, a new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or timed out. If a ZSK is suspected of having been compromised or revealed to unauthorized parties, this will be notified through the communication channels indicated in Section 2.1.

- If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruption in relation to the risk that the compromised key presents. A KSK rollover in progress is always notified through the channels indicated in Section 2.1.

- If a KSK is lost, a new key will be generated and a key exchange will take place without an overlap between the lost and the new KSK. At such time, that will be announced through the channels indicated in Section 2.1. During the time until the rollover, the key set will remain static and any scheduled ZSK rollover will be postponed until after the KSK exchange.

4.6.4. Business Continuity and IT Disaster Recovery Capabilities

NZRS has a contingency plan that ensures the operation of critical production systems can be relocated between the two operation facilities within minutes. The facilities are equivalent in terms of physical and logistical protection. Information is replicated between the facilities.

The contingency plan and routines are regularly tested. The completed tests and trials are recorded and subsequently evaluated.

The contingency plan includes:

- Who decides on the activation of an emergency recovery procedure.
- How and where the crisis management shall convene
- Activation of backup operations
- Criteria for restoring normal operations

4.7. Entity Termination

If NZRS must discontinue DNSSEC for the .nz zone for any reason and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed. If operations are to be transferred to another party, NZRS will participate in the transition to make it as smooth as possible.

5. Technical Security Controls

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Key generation takes place in a hardware security module (HSM) that is managed by trained personnel in trusted roles.

Key generation takes place when the initial signing setup is being prepared and during the execution of the Key Generation Procedure. One SA, and two KSO working coordinately and present during the entire operation must perform these processes.

The entire key generation procedure is logged, part of which is done electronically and part of which is done manually on paper by the KGA. Both components of the execution log will be published afterwards according to Section 2.2.

5.1.2. Public key distribution

See Section 2.2.

5.1.3. Public key parameters generation and quality checking

Key parameters are regulated by .NZ's KASP (Key and Signature Policy) and quality control includes checking the key length.

5.1.4. Key usage purposes

Keys generated for DNSSEC are not used for any other purpose or outside the signing system. The maximum validity period for a signature created by a DNSSEC key is 16 days, and this validity period always begins when the signature has been established. Signatures are recalculated 3 days before their expiration.

5.2. Private key protection and Cryptographic Module Engineering Controls

All cryptographic functions involving the private component of the ZSK and KSK are to be performed within the HSM; that is, the private component cannot be exported from the HSM except in encrypted form for purposes of key backup.

5.2.1. Cryptographic module standards and controls

The system uses a hardware security module (HSM) which conforms to the requirements in FIPS 140-2 Level 3.

5.2.2. Private key (m-of-n) multi-person control

During the HSM activation, all Keystore Security Officers and Device Security Officers need to be present to be enrolled as such and activate the HSM. One System Administrator is required to get logical access. Multi-person control will be applied during the creation of a key backup and restoration.

5.2.3. Private key escrow

Private components of .nz Zone and Key Signing Keys are not escrowed.

5.2.4. Private key backup

NZRS creates backup copies of .nz ZSK and KSK private keys for routine recovery and disaster recovery purposes. One copy will be held on each production site, plus a copy in an off site location. All backup copies are encrypted.

Keys are stored in an encrypted format on the signing module's hard drive. The encrypted key archive is securely backed up and synchronized between the operations facilities shortly after key generation.

5.2.5. Private key storage on cryptographic module

Private keys held on hardware cryptographic modules are stored in encrypted form.

5.2.6. Private key archival

ZSK key pairs do not expire. Superseded key pairs will be securely retained for a period of at least 7 days using hardware security modules that meet the requirements of this DPS. These key pairs will not be used for any signing events after their supersession.

5.2.7. Private key transfer into or from a cryptographic module

For Disaster Recovery Policy, the private keys are copied from one facility to the other in encrypted form. The key export and import process must be executed by one at least one System Administrator and at least two Keystore Security Officers working coordinately.

5.2.8. Method of destroying private key

After their useful life, keys are removed from the signing system. Where required, NZRS destroys the keys utilizing the zeroize function of its HSM.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

Public keys are archived in accordance with the archiving of other information relevant to traceability in the system, such as log data.

5.3.2. Key usage periods

Keys become invalid as they are taken out of production. Old keys are not reused.

5.4. Activation data

Private keys are put in production during the Key Generation Procedure, requiring the presence of at least one System Administrator and two Keystore Security Officers to proceed.

5.4.1. Other aspects of activation data

In the event of a crisis situation, there is a sealed envelope in a secure location that contains activation information as part of a Disaster Recovery Kit. NZRS contingency plan procedures indicate the conditions in which this shall be applied.

5.5. Computer Security Controls

All critical components of NZRS's systems are placed in the organizations secure facilities in accordance with NZRS Security Policy and Procedures. Access to the server's operating systems is limited to individuals that require this for their work, such as system administrators and operators.

5.6. Network Security Controls

NZRS has logically separated networks that are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. All sensitive information that is transferred over the communication networks is always protected by strong encryption.

5.7. Time stamping

NZRS retrieves time from trusted Stratum 1 NTP timeservers. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

All applications are developed and implemented by NZRS in compliance with NZRS Change Policy.
This includes mandatory use of version control system, regression testing, and isolated testing environment.

5.8.2. Security management controls

NZRS has mechanisms to control and monitor the configuration of its systems and to validate the software packages installed preserve their integrity.

6. Zone Signing

The signing process is conducted automatically each hour on the hour. If no changes are produced between hours, the previous zone is preserved and only the signatures close to expiration will be regenerated.

6.1. Key lengths and algorithms

Key pairs are required to be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

The current KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits.
The current ZSK key pair(s) is an RSA key pair, with a modulus size of 1024 bits.

6.2. Authenticated denial of existence

Authenticated denial of existence will be provided through the use of NSEC records as specified in RFC 4034 for the .nz zone, and NSEC3 records as specified in RFC 5155 for the second level zones.

6.3. Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA-256 (RSA/SHA-256, RFC 5702).

6.4. Zone signing key roll-over

ZSK rollover is carried out every 3 months in a semi-automated procedure.

6.5. Key signing key roll-over

Each KSK will be scheduled to be rolled over through a key ceremony each year, and extraordinarily when needed as described in Section 4.6.3.

6.6. Signature life-time and resigning frequency

RRsets are signed with the ZSKs with a validity period of 12 to 16 days. Resigning takes place every hour, but only signatures close to expiration will be regenerated. Signatures are recalculated when their expiration date is less than 3 days in the future.

6.7. Verification of zone signing key set

Security controls are conducted on the DNSKEY records before publishing to ensure correct signatures and validity periods. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the .nz SOA.

6.8. Verification of resource records

NZRS verifies that all resource records are valid according to the current standards prior to distribution.

6.9. Resource records time-to-live

RR type	TTL
DNSKEY	24 hour
NSEC	1 hour
NSEC3	1 hour
Delegation Signer (DS)	24 hours
RRSIG	varies, depending on the RRset signed

7. Compliance Audit

7.1. Frequency of entity compliance audit

NZRS annually engages external auditors to check on compliance with the security policy and procedures. The annual security audit work item is detailed in the NZRS Board Audit & Risk Committee annual work program and the terms of reference for each audit are signed off by the committee.

Additional audits may be required at any time under the following circumstances:

- Recurring anomalies
- Major changes to management, organization or processes

7.2. Identity/qualifications of auditor

The auditor must be able to demonstrate proficiency with IT security tools, security auditing, DNS and DNSSEC.

7.3. Auditor's relationship to audited party

An external auditor will be appointed for the audit. When necessary the auditor shall be able to recruit specific expert knowledge. The auditor is responsible during the entire auditing process.

7.4. Audit scope

The scope of the audit will always include the following DNSSEC components:

- Key Management Operation
- Infrastructure Controls
- Signing Lifecycle
- Practices Disclosure

The following items have been performed in previous audits and will continue to be included on a regular basis with future audits:

- Internal security control evaluation
- Penetration testing
- Procedural compliance
- Security culture evaluation
- Application vulnerability assessment
- Offsite backup procedures

7.5. Actions taken as a result of deficiency

If any anomaly or deficiency is detected, the auditor shall immediately notify NZRS verbally. NZRS Management then will determine the course of action to prepare and execute a corrective action plan.

7.6. Communication of results

The auditor shall provide a written report of the audit results to NZRS not later than 30 days after the audit.