

APNIC DNSSEC

Policy and Practice Statement

Table of Contents

Overview	4
Document name and identification	4
Community and applicability	4
Specification administration	4
Specification administration organization	4
Contact information	4
Specification change procedures	4
Repositories	5
Publication of public keys	5
Registration of delegation signer (DS) resource records	6
Method to prove possession of private key	6
Removal of DS resource records	6
Who can request removal	6
Procedure for removal request	6
Emergency removal request	6
Physical controls	7
Site location and construction	7
Physical access	7
Power and air conditioning	7
Water exposures	7
Fire prevention and protection	7
Media storage	7
Off-site backup	7
Procedural control	7
Trusted Roles	7
Number of persons required per task	7
Personnel controls	7
Qualifications, experience, and clearance requirements	7
Training requirements	8
Job rotation frequency and sequence	8
Contracting personnel requirements	8
Documentation supplied to personnel	8
Audit logging procedures	8
Types of events recorded	8

Compromise and disaster recovery	8
Incident and compromise handling procedures	8
Entity private key compromise procedures	8
Key pair generation and installation	9
Key pair generation	9
Public key delivery	9
Key usage purposes	9
Private key protection and cryptographic module engineering control	9
Cryptographic module standards and controls	9
Private key (m-of-n) multi-person control	9
Private key escrow	9
Private key backup	9
Private key storage on cryptographic module	9
Private key archival	9
Private key transfer into or from a cryptographic module	9
Method of activating private key	10
Method of deactivating private key	10
Method of destroying private key	10
Other aspects of key pair management	10
Key pair usage	10
Key pair lifecycle states	10
Computer security controls	10
Network security controls	10
Time stamping	10
Life cycle technical controls	10
Key lengths, key types, and algorithms	11
Key Signing Key	11
Zone Signing Key	11
Authenticated denial of existence	11
Signature format	11
Key rollover	11
Key Signing Key rollover	11
Zone Signing Key rollover	11
Signature lifetime and re-signing frequency	11
Resource records time-to-live	11

Frequency of entity compliance audit	12
Identity/qualifications of auditor	12
Actions taken because of deficiency	12

Introduction

APNIC is the Regional Internet Registry for the Asia Pacific region, responsible for allocating Internet number resources such as IP addresses and AS numbers. APNIC is also responsible for operating reverse Domain Name System (DNS) zones for the IP address blocks that have been allocated. This DNSSEC Policy and Practice Statement (DPS) applies to Reverse DNS zones that APNIC is responsible for publishing in the DNS.

Overview

Domain Name System Security Extensions (DNSSEC) allow the Internet community to validate that APNIC reverse zone data has not been modified in transit. This DPS describes how APNIC operates and maintains the DNSSEC operation of the reverse zones. The following itemized list follows the standard DPS template (RFC 6841).

Document name and identification

APNIC DNSSEC Policy and Practice Statement (DPS).

Community and applicability

The zones administered by APNIC.

Specification administration

This document (DPS) will be reviewed and updated periodically as required.

Specification administration organization

APNIC Pty Ltd

Contact information

Network Infrastructure Services

35 Boundary Street
South Brisbane
4101 QLD Australia

email: dns-ops@apnic.net

Specification change procedures

Any changes to this document need to be reviewed and approved by the APNIC Infrastructure Services Manager, Technical Director and Deputy Director General.

Publication and repositories

Repositories

DNSSEC relevant information is published on the APNIC website:

<https://www.apnic.net/manage-ip/apnic-services/dnssec>

Publication of public keys

The current Key Signing Keys (KSKs) are used to generate DS records, which are lodged in the parent zones and signed over using their operational keys. No other external publication of the APNIC KSK takes place.

Operational requirements

Registration of delegation signer (DS) resource records

During a key rollover event in a specific child zone, a chain of trust can be created by registering DS-RDATA from a domain object in the APNIC Whois Database. The process of registering DS-RDATA is documented in the APNIC website in the section “How can you update domain objects in MyAPNIC” (<https://www.apnic.net/manage-ip/apnic-services/dnssec>).

Method to prove possession of private key

At the start of a rollover event, the new KSKs are published in the zone where the signature was validated. Validation is also done if this was signed by the active KSKs.

Removal of DS resource records

DS record removal for any specific child zone is the responsibility of the Local Internet Registry using the MyAPNIC web portal. DS record removal from the parent zone is done during the KSK rollover event for the parent zone.

Who can request removal

Any user with valid credentials in MyAPNIC that permits edits of the child zones whois data can request removal.

Procedure for removal request

Please login to MyAPNIC and navigate to the “Whois Update” section to lodge your removal request.

Emergency removal request

Please contact the APNIC Helpdesk to lodge an emergency removal request.

Facility, management, and operational control

Physical controls

Site location and construction

APNIC uses two commercial data centres to operate core APNIC services that implement DNS primary and DNSSEC signing along with the MyAPNIC web portal.

Physical access

Only authorized Trusted Role personnel have access to APNIC’s restricted facilities. The facilities are constantly monitored, with entry and exit logging.

Power and air conditioning

The commercial data centres that APNIC uses are properly air-conditioned and have redundant systems in place if a power failure occurs.

Water exposures

APNIC's facilities and facilities used by APNIC are above ground level to avoid risk of water exposure.

Fire prevention and protection

All facilities are equipped with fire suppression and monitoring, including distributed fire alarm controls.

Media storage

Only encrypted system key backups are stored outside of the signer systems.

Off-site backup

In addition to the APNIC internal storage system, encrypted media is also stored in an off-site facility.

Procedural control

Trusted Roles

There is one designated team responsible for DNSSEC operations.

Number of persons required per task

Two senior Trusted Role members are required to validate change request prior to any changes. Two senior Trusted Role members work as a pair to perform the key rollover.

Personnel controls

Qualifications, experience, and clearance requirements

A team member of these Trusted Roles must have been working in APNIC DNS operations for more than a year.

Training requirements

A new team member must attend at least one key rollover event as an observer before performing the DNSSEC operation task.

Job rotation

DNSSEC key rollover events are rotated amongst Trusted Role members to share knowledge and experience.

Contracting personnel requirements

The DNSSEC signer is only accessible to a Trusted Role. An authorized team member will perform any contractor or consultant work.

Documentation supplied to personnel

The DNSSEC operational documentation is available to all Trusted Role members. The entire team reviews this document regularly.

Audit logging procedures

Types of events recorded

Entry and exit to and from the signer facilities are logged. Site access requires prior authorization. Events on the signer system are logged and archived regularly. KSK rollover events are logged and archived.

Compromise and disaster recovery

Incident and compromise handling procedures

Where the security of the system is possibly compromised, an operational incident will be reported and investigated. The entire team will conduct the investigation.

If the private key has been compromised there will be an emergency rollover operation.

Entity private key compromise procedures

If the private key has been compromised, the team will raise a change request for an emergency rollover. After the rollover, the previous key will only be kept in the system for the duration of DNSKEY TTL.

Technical security controls

Key pair generation and installation

Key pair generation

A pair of KSK and ZSK will be generated by the signer during key rollover events.

Public key delivery

Public keys are published as DNSKEY resource records to the zone by the signer on each key rollover event.

Key usage purposes

A pair of keys is used for one zone only, these keys are never recycled or reused after each rollover.

Private key protection and cryptographic module engineering control

Cryptographic module standards and controls

The signer supports range of DNSSEC algorithms defined by IETF standards. These algorithms are implemented using standard cryptographic libraries. The system provides automatic key lifecycle management. If required, the signer supports a PKCS #11 interface allowing integration with Hardware Security Modules (HSM).

Private key access control

While private keys are readable from the signer system, access to the signer system is governed by the Trusted Role.

Private key escrow

No private key escrow is being used.

Private key backup

The signer system creates an encrypted backup of the private key database after each re-signing event.

Private key storage on cryptographic module

The signer system uses a software-based cryptographic module to maintain DNSSEC keys and is protected by multi-factor authentication.

Private key archival

Used private keys are not archived in the system after each rollover event. Private keys can be restored from an encrypted backup (see above).

Private key transfer into or from a cryptographic module

Private keys can only be transferred and decrypted by a Trusted Role into another preconfigured trusted backup signer of the same architecture.

Method of activating private key

After each rollover event, the signer generates a new key and activates it for double signing.

Method of deactivating private key

A private key can only be deactivated or removed after a scheduled or emergency rollover event.

Method of destroying private key

The signer system automatically deletes private keys from the database after a rollover has been completed.

Other aspects of key pair management

Key pair usage

KSKs are rolled over annually and ZSKs are rolled over every 3 months.

Key pair lifecycle states

States of key being rolled-in

- **Published** - The key is published in the zone but not used for signing.
- **Active** - The key is used for signing.
- **Ready (only for KSK)** - The key is published in the zone and used for signing. The old key is still active while waiting for the DS records in the parent zone to be updated.

States of key being rolled-out

- **Retire-active** – The key is still used for signing and is published in the zone waiting for the updated DS records in the parent.
- **Retired** – The key is no longer used for signing.
- **Removed** – The key is not used in any way.

Computer security controls

APNIC ensures that access to the signing system is only permitted to designated Trusted Roles.

Network security controls

The signer system is split into two separate private VLANs for redundancy. DNS operations to the signer systems are limited to known hosts that are required for normal operations.

Time stamping

The signer system maintains an accurate time against an internal trusted NTP source.

Life cycle technical controls

Software updates and configuration changes are tested against a backup signer system before being deployed into the production signer system.

Zone signing

Key lengths, key types, and algorithms

Key Signing Key

We use ECDSAP256SHA256 with 256-bit length. **Zone**

Signing Key

We use ECDSAP256SHA256 with 256-bit length.

Authenticated denial of existence

The use of NSEC records in the zone provides authenticated denial of existence.

Signature format

The generated signature uses ECDSA SHA256 hash.

Key rollover

Key Signing Key rollover

At the start of rollover event, we use the double signing scheme that is documented in RFC 4641.

Zone Signing Key rollover

We use the pre-publish scheme to rollover the ZSK that is documented in RFC 4641.

Signature lifetime and re-signing frequency

Zones are signed every 7 days with a 15-day signature validity.

Resource records time-to-live

The DNSKEY KSK TTL is equal to 1 hour.

The DNSKEY ZSK TTL is equal to 1 hour.

The NSEC TTL is equal to 1 hour.

The RRSIG TTL is equal to 1 hour.

The DS TTL is equal to 24 hours.

Compliance audit

APNIC will be able contract an external company to audit the DNSSEC operations within the scope of this DPS document.

Frequency of entity compliance audit

The compliance audit will be conducted as required.

Identity/qualifications of auditor

The identity of the contracted auditor will be published along with the result of audit.

Actions taken because of deficiency

The audit result will be published along with any the action taken.

Version	Date	Author	Changes Made
1.0	2021-06-16	Arth Paulite	Initial document
2.0	2025-11-05	Arth Paulite	Operational changes for different signer
3.0	2026-08-26	Arth Paulite	Postal address change