APNIC DNSSEC

Policy and Practice Statement

APNIC

Table of Contents

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

6 Cordelia Street

South Brisbane

Australia 4101 QLD

email: dns-ops@apnic.net

Specification change procedures

Any changes to this document needs 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 during office hours 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 master and DNSSEC signing along with the MyAPNIC web portal.

Physical access

Only authorized APNIC Infrastructure Services 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 on offline media.

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 are two designated teams responsible for DNSSEC operations. Each team has two persons with separate roles.

Number of persons required per task

Both teams are required to validate change requests and a single team is required to perform the approved operations.

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 frequency and sequence

DNSSEC key rollover events are rotated between the two teams to avoid a single team from performing two consecutive rollover operations.

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 the member of a Trusted Role. 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 pool of keys is generated by the signer system for both KSK and Zone Signing Keys (ZSKs) using the host's Trusted Platform Module chip (TPM).

Public key delivery

Copies of the public keys are retrieved from the signer system and compared against DNSKEY keys in the zone before publishing.

Key usage purposes

Each zone has two pairs of KSKs and ZSKs; one is active while the other pair is on stand-by. 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 system complies with FIPS 140-2, level 2 certification.

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

Private keys are not 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 hardware TPM crypto chip to generate and maintain private encryption keys that never leave the chip itself.

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 cloned and transferred in an encrypted form into another preconfigured trusted backup signer of the same architecture.

Method of activating private key

After each rollover event, the signer picks a new key from a pool and activates it as a standby key.

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 monthly.

Key pair lifecycle states

The stand-by KSK and ZSK are not published in the zone, and will change to active after each rollover.

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. Connections to the signer systems are limited to a known host that is required for the 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 daily with a 30-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 1 day.

Compliance audit

APNIC will 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 annually.

Identity/qualifications of auditor

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

Actions taken as a result of deficiency

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