Netnod DNSSEC Policy and Practice Statement

Introduction

Overview

The purpose of this document is to enable stakeholders to determine the level of trust they wish to grant to Netnod DNSSEC management. It details the procedures and policies employed by Netnod in operating those zones for which it offers DNSSEC signing service.

This document conforms to the IETF Internet draft for a DNSSEC Practice Statement, or DPS (see: RFC 6841).

Applicability

The following functional subsets of the community to which this document has applicability have been identified.

Customer

All zones covered by this document originate from Netnod customers. The zones provided by customers are correct, but unsigned, DNS-zones. The zones are transferred by the customer to Netnod via TSIG signed zone transfers.

Zone administrator

The entity responsible for receiving and properly ensuring that Delegation Signer (DS) Resource Records provided by Netnod are entered into parent zones. This could be the same entity as the customer or a separate entity.

Specification Administration

This DPS will be periodically reviewed and updated, as appropriate, initiated by Netnod's CSO, and determined by Netnod's CTO.

Specification administration organisation

Netnod AB (Netnod)

Contact Information

Greta Garbos väg 13
SE-169 40 Solna
Sweden

Email: noc@netnod.se

Specification Change Procedures

Any change to this document needs to be signed off by Netnod's CSO and CTO.

Publication and Repositories

Repositories

Information about the DNSSEC public keys used to sign the zones, for which Netnod systems are authoritative, is provided via a TLS secured website.

Publication of Key Signing Keys (KSK)

Netnod will publish its public Key Signing Keys in the form of DS records.

Delegation Signer (DS) Format

In this format, the public key is presented in a hash representation according to the DS Resource Record specification.

Access Controls on Repositories

Information published in the DNSSEC repository is intended to be available to the general public, and can be validated through regular DNSSEC.

Operational Requirements

Registration, Modification and Removal of Delegation Signer (DS) Resource Records

DNSSEC for a child zone is activated by publishing a signed DS record for that zone. Netnod by default provides DS records to the zone administrator for publication in the parent zone.

Method to Prove Possession of Private Key

Netnod provides DS records matching DNSKEY records added to zones to zone administrators according to agreement.

Facility, Management and Operational Controls

Physical Controls

Site location and construction

Netnod operates multiple sites in Sweden. These include server rooms in multiple communications bunkers of military grade. DNSSEC-related activities are performed only at these secure facilities.

Physical access

All of our facilities have restricted access, limited to authorised personnel.

Power and Air Conditioning

All relevant facilities have Uninterruptible Power Supply (UPS) capabilities and air conditioning. The external data centre sites have redundant systems in place in the event of a power failure.

Water Exposure

Relevant facilities implement flood protection and detection mechanisms.

Fire Prevention and Protection

All facilities have fire detectors, fire prevention and / or protection systems.

Media Storage

Sensitive media is stored in a safe which is only accessible by Netnod Senior Management and specifically designated personal.

Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information is rendered unreadable before disposal.

Off-site Back-up

Signer backups are stored on our storage systems spread across our data centers.

Procedural Controls

Trusted Roles

Trusted roles include all employees that have access to or control cryptographic operations that may materially affect:

- Generation and protection of private part of KSK and ZSK
- Generation and signing of Zone file data

Trusted roles include, but are not limited to:

- Senior DNS staff
- Senior Security staff

Tasks Requiring Separation of Duties

Any task performed on the signer systems requires at least one Senior DNS staff and one Senior Security staff to be present, where one acts as an observer.

Personnel Controls

Qualifications, Experience and Clearance Requirements

Engineers taking part in the *Trusted Roles* have to have been working for the company for no less than one year and must have the qualifications necessary for the job role.

Netnod employs background checks and verification of statements at the time of employment.

Training Requirements

New senior staff have to observe at least one regular key roll-over before conducting signing tasks.

Job Rotation Frequency and Sequence

No single individual can perform a role in a regular key roll-over more than three times in a row. This is to ensure redundancy of competence.

Contracting Personnel Requirements

No person outside of the specified *Trusted Roles* can get access to the signer systems.

Documentation Supplied to Personnel

The regular procedures for backup and restore are available to all personnel involved. If major alterations to those procedures are made, the engineers of those teams will be informed accordingly.

Audit Logging Procedures

Types of Events Recorded

Physical access to the facilities used for our signing systems is logged automatically on enter and exit. The main operation site requires personnel to be specifically granted permission to enter the suite in which the equipment is located and they will have to sign-in using a valid entry token.

Log messages from the signer systems will be sent securely to a write-once logging system and recorded for audit purposes.

Protection of Audit Log

Audit logs of our main operation site are kept in a separate audit cluster. Access to the audit logs of our own facilities is only available to the operations department.

Compromise and Disaster Recovery

Any relevant events relating to the secure operation of Netnod signing-systems will be announced to relevant stakeholders.

Incident and Compromise Handling Procedures

If an event leads to, or could lead to, a detected security compromise, it is treated as an incident and handled in accordance with Netnod incident management processes.

Entity Private Key Compromise Procedures

Any suspected or known compromise of ZSK will lead to immediate removal and replacement of ZSK.

Any suspected or known compromise of KSK will lead to as soon as possible executing a controlled key rollover.

Technical Security Controls

Key Pair Generation and Installation

Key Pair Generation

Key Signing Key (KSK) are generated on the signer systems using secure elements. Zone Signing Key (ZSK) are generated similarly and can be stored on encrypted storage.

Public Key Delivery

The public key is retrieved from the signer system and then published as detailed in the section *Publication and Repositories*.

Key Usage Purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing systems.

Private Key Protection and Cryptographic Module Engineering Controls

Cryptographic Module Standards and Controls

Systems used for signing with KSK are FIPS 140-3 Level 3-certified.

Private Key (m-of-n) Multi-person Control

No access to unencrypted KSK is available in the entire system. Access to the signer system is specified in the *Trusted Roles* section.

Private Key Backup

The signer system pushes a back-up, including ZSK, onto our storage system. This back-up is encrypted. Access to the back-up archives is limited to persons designated by Senior Management.

KSK are only backed-up on hardware based HSMs.

Private Key Archival

Private ZSKs can be restored from the back-ups specified above. Private keys are not archived on the signer system once they have been revoked.

Private KSKs can be synchronized between hardware based HSMs, and are never present outside of the HSM modules in unencrypted form.

Private Key Transfer Into or From a Cryptographic Module

Private keys can only be transferred off the system in encrypted form and restored onto the back-up system by the teams described in the *Trusted Roles* section.

Other Aspects of Key Pair Management

Public Key Archival

We are only publishing the public keys currently relevant to the operation of our customers zones. No archive of public keys past their revocation is available.

Key Usage Periods

KSKs will be rolled over every other year and ZSKs will be rolled over quarterly, or as stated by contract with the customer.

Computer Security Controls

Netnod ensures that the systems maintaining key software and data files are Trustworthy Systems secure from unauthorized access. In addition, Netnod limits access to production servers to those individuals with a valid reason for such access. Netnod employees in general do not have accounts on production servers.

Network Security Controls

Systems holding the signing infrastructure are inside a dedicated VLAN inside our network infrastructure. The only communications channel to those systems is through our firewall, which is limited to the minimal capabilities necessary for the operation of the system.

Timestamping

The signer systems use time traceable to UTC(sp) directly, and UTC over time.

Life Cycle Technical Controls

System Development Controls

We are using a third-party solution on our signer systems. We test new releases of this software in a lab environment provided by our supplier. Once these tests are concluded successfully, we do a staged roll-out of the new release onto our inactive signer system first, and then onto our active signer system.

Zone Signing

Key Lengths and Algorithms

Key Signing Key

We use algorithm 15 (ED25519) as the default generation algorithm, or as stated by contract with the customer.

Zone Signing Key

We use algorithm 15 (ED25519) as the default generation algorithm, or as stated by contract with the customer.

Pre-signing and post-signing validation

Zones will be validated prior to signing to follow applicable DNS standards, or by method as stated by contract with the customer. Zones will also be validated after signing to follow applicable DNS- and DNSSEC standards, or by method as stated by contract with the customer.

Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC or NSEC3 per customer requirements.

Signature Format

Our signatures are created with the SHA256 hash using RSA.

Zone Signing Key Roll-over

We will roll the ZSK with a pre-publishing scheme as described in RFC 6781, section 4.1.1.1.

Key Signing Key Roll-over

We will roll the KSK with a double-signing scheme as described in RFC 6781, section 4.1.1.2.

Signature Life-time and Re-signing Frequency

We re-sign our zones daily with a signature lifetime of 30 days.

Resource Records Time-to-live

Record type	TTL
DNSKEY	Equal to the TTL used for the SOA record
NSEC	Equal to the minimum field of the SOA record
RRSIG	Equal to the lowest TTL of the record set covered
DS	Equal to the TTL of the NS RRset