DNSSEC Policy Statement – Version 1.1.0

This DNSSEC Practice Statement (DPS) conforms to the template included in RFC 6841.

1. Introduction

The approach described here is modelled closely on the corresponding DPS procedures published for .SE by the "Stiftelsen för Internetinfrastruktur" (.SE The Internet Infrastructure Foundation)[1] and the DPS procedures published for the .CA by the Canadian Internet Registration Authority (CIRA)[2].

1.1. Overview

DNSSEC is an extension to the DNS that allows data retrieved from the DNS to be authenticated. DNSSEC is specified in RFC 4033, RFC 4034, RFC 4035,RFC 5155 and RFC 5702. DS Resource Record updates to the root zone for TLDs will conform to the process as described by IANA.

1.2. Document Name and Identification

Document Name: CentralNic DPS Statement
Version: 1.1.0
Last Modification: 2013-12-16
Document Available From: https://www.centralnic.com/registry/dnssec/dps
Contact: Gavin Brown

1.3. Community and Applicability

1.3.1. Registry

CentralNic operates registry system for various ccTLDs, gTLDs and ccSLDs. CentralNic is responsible for the management of the registry, and consequently for the registration of domain names under various top-level domains. CentralNic is responsible for all DNSSEC operations of these zones.

1.3.2. Registrars

A registrar is a party responsible for requesting changes in the registry on behalf of registrants. Each registrar is responsible for the secure identification of the registrant of a domain name under its sponsorship. Registrars are responsible for adding, removing or

[1] https:/www.iis.se/docs/se-dnssec-dps-eng.pdf
[2] http://cira.ca/knowledge-centre/technology/dnssec/practice-statement/

updating Delegation Signer (DS) records for each domain at the request of the domain's registrant.

1.3.3. Registrants

Registrants are responsible for generating and protecting their own keys, and registering and maintaining corresponding DS records through a registrar.

1.3.4. DNS Operators

The registrant may outsource their technical responsibility to a third-party DNS Operator.

1.3.5. Relying Party

The relying party is the entity that makes use of DNSSEC signatures, such as DNSSEC validators and other applications. Relying parties should make use of a root zone trust anchor to obtain the trust anchors for the various zones via publication of the DS record.

1.3.6. Applicability

This DPS applies to all top-level and second-level domains operated by CentralNic.

1.4. Specification Administration

This DPS is updated as appropriate with best practices in the industry.

1.4.1. Specification Administration Organisation

CentralNic Ltd, 35-39 Moorgate, London, EC2R 6AR, United Kingdom.

1.4.2. Contact Information

Operations Team, CentralNic Ltd, 35-39 Moorgate, London, EC2R 6AR, United Kingdom. Email dnssec@centralnic.com

1.4.3. Specification Change Procedures

The current version of this document is available at:

https://www.centralnic.com/registry/dnssec/dps

CentralNic may amend the DPS without notification for changes, but will provide reasonable notice of significant changes. All changes to this DPS will be effective immediately upon publication.

2. Publication and Repositories

Notifications relevant to DNSSEC at CentralNic will be distributed by e-mail to CentralNic registrars and the dns-operations mailing list[3].

2.1. Repositories

CentralNic publishes DNSSEC-related information to the general public at:

https://www.centralnic.com/registry/dnssec

2.2. Publication of public keys

CentralNic publishes Key Signing Key (KSK) for its zones as DS records in the root zone. Historic key information will be published at:

https://www.centralnic.com/support/dnssec

3. Operational Requirements

3.1. Meaning of Domain Names

For the purposes of this document, a domain name is a name registered under a top-level domain (ccTLD such as .LA, gTLD such as .WIKI) or second-level domain (ccSLD such as .UK.COM), and corresponds to a delegation from the parent zone to name servers operated for the domain name's registrant.

3.2. Identification and Authentication of Child Zone Manager

Identification and authentication of each child zone manager is the responsibility of the sponsoring registrar for the domain name.

3.3. Registration of delegation signer (DS) resource records

The registry accepts DS records through an RFC 5910 EPP interface and via the Registrar Console[4]. The registry will accept any syntactically valid DS record, and no checks will be performed as to the accuracy of the trust anchor with respect to the child zone's KSK to allow pre-publishing of DS records.

[3] https:/lists.dns-oarc.net/mailman/listinfo/dns-operations
[4] https://registrar-console.centralnic.com

3.4. Method to Prove Possession of Private Key

The sponsoring registrar for a domain name is responsible for authenticating the registrant as the manager of the domain name in control of the private key.

3.5. Removal of Delegation Signer Record

DS records are removed from the registry using an EPP interface according to RFC 5910 or manually via the CentralNic Registry web interface.

3.5.1. Who can request removal

The registrant has the authority to request removal of a DS record, subject to identical authentication as required for modifications of NS records.

3.5.2. Procedure for removal request

The registrant of a domain name requests the domain's sponsoring registrar to remove the DS record. The registrar transmits this request to the registry using EPP or the Registrar Console. Once the transaction has been successfully received and processed by the registry, the DS record will be removed from the zone when the following revision of the zone is distributed (no later than 60 minutes after). The sponsoring registrar must comply with requests from the registrant, regardless of the standing between the two parties.

3.5.3. Emergency removal request

There is no provision for emergency removal requests.

4. Facility, Management and Operational Controls

4.1. Physical Controls

CentralNic has implemented a Security Policy, which supports the security requirements of this DPS.

4.1.1. Site Location and Construction

CentralNic has established two fully operational and geographically dispersed operation centres. Both sites are protected by multiple tiers of physical security that deter, prevent and detect unauthorized access attempts. Each site contains a full set of equipment necessary to sign and validate all zones. All signing components are placed within locked cabinets. A third site is used to store off-line HSMs and associated portable media, within a secure container.

4.1.2. Physical Access

Physical access to operation centres is restricted to authorized personnel. Access is controlled using RFID photo cards and visual confirmation of identity by security personnel. Technical areas are further controlled by PIN entry locks on doors. Access to locked cabinets is further restricted to personnel with trusted roles. The physical security system includes additional tiers of key management security and segregation of duties to protect both online and offline storage of HSMs and keying material.

Offline HSMs are protected through the use of locked cabinets.

4.1.3. Power and Air Conditioning

Operation centers are equipped with redundant power sources and air conditioning systems to ensure a consistent, stable operating environment.

4.1.4. Water Exposure

Both operation centers implement flood protection and detection mechanisms.

4.1.5. Fire Prevention and Protection

Operation centers are equipped with fire detection and extinguishing systems.

4.1.6. Media Storage

All media containing production software and data, audit, archive, or backup information is stored securely within the operation centers

4.1.7. Waste Disposal

Sensitive media and other material that may contain sensitive information are destroyed in a secure manner, either by CentralNic or by a contracted party.

4.1.8. Off-Site Backup

CentralNic performs regular backups of critical data, audit logging data and other sensitive information. An off-site facility is leveraged for storage of backup media. Physical access to the storage facility is limited to authorized personnel.

4.2. Procedural Controls

4.2.1. Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control operations that may materially affect DNSSEC content.

Trusted Persons include; but are not limited to:

- DNS Operations personnel
- Security personnel
- System administration personnel
- Executives that are designated to manage infrastructure

Trusted positions are assigned to CentralNic staff personnel. The trusted roles are:

- "SA" - System Administrator
- "SO" - Security Officer
- "WI" - Witness

There must be at least two different individuals assigned to each position.

4.2.2. Number of Persons Required per Task

- HSM Activation and Deactivation: 3 persons (1 SA, 1 SO, 1 WI)
- Key Generation: 3 persons (1 SA,1 SO,1 WI)
- Distribution of encrypted Key Archives to: 2 persons (1 SA or SO, 1 WI)
- Signing Components: 2 persons (1 SA and 1 SO or WI)
-

4.2.3. Identification and Authentication for Each Role

Only CentralNic staff members who have signed a CentralNic employment agreement may hold a trusted person role of SO or SA. The role of WI can be filled with any person of good standing. Valid identification must be provided.

4.2.4. Tasks Requiring Separation of Duties

Tasks requiring separation of duties include, but are not limited to, the generation, implementation or destruction of DNSSEC key material. No two trusted roles may be held by a single individual.

Systems Administrators have exclusive physical access to DNSSEC operational equipment. Security Officers and Witnesses have no such access. Security Officers hold credentials for HSM activation. Systems Administrators hold no such credentials. A Witness is a person in good standing with no ties to the operations, or IT aspects of the company. The witness has the ability to question the procedure at all stages of DNSSEC procedures..

4.3. Personnel Controls

4.3.1. Qualifications, Experience and Clearance Requirements

Candidates for any trusted role must demonstrate appropriate background knowledge and qualifications.

4.3.2. Background Check Procedures

Background checks for candidates for SA and SO roles are carried out by the Human Resources department at CentralNic, and follow normal procedures for background checks on new hires. The witness has to be a person in good standing.

4.3.3. Training Requirements

CentralNic provides its personnel with training upon hire as well as on-going training as needed to perform their job responsibilities competently and satisfactorily.

4.3.4. Job rotation frequency and sequence

SA and SO roles are kept as stable and with the least amount of rotation possible by assignment to senior staff members where possible

4.3.5. Sanctions for unauthorized actions

Any unauthorized action taken by a staff member will result in disciplinary action and possible criminal prosecution.

4.3.6. Contracting personnel requirements

Personnel hired by CentralNic as contractors are subject to background checks and confidentiality agreements. Contractors must demonstrate appropriate qualifications.

4.3.7. Documentation supplied to personnel

Personnel will be supplied with documentation required for their trusted role, including this DPS policy, audits performed in the past, plus all system administration documentation relevant to the DNSSEC signing solution.

4.4. Audit Logging Procedures

CentralNic implements automatic log collection from CentralNic computer systems. Paper documentation relating to the execution of procedures is also collected for the purposes of auditing performance of those procedures.

4.4.1. Types of Events Recorded

CentralNic manually or automatically logs critical events related to KSK and ZSK management.

CentralNic manually or automatically logs critical events related to system security and management.

Log entries include the following elements:

- Date and time of the entry based on NTP
- Identity of the entity making the journal entry
- Serial or sequence number of entry, for automatic journal entries
- Entry type and log level
-

4.4.2. Frequency of Processing Log Information

Logs are continuously analyzed through automatic and manual controls.

4.4.3. Retention Period for Audit Log Information

Electronic logs are retained on-line for one year. All log information collected is archived for at least three years.

4.4.4. Protection of Audit Log

All audit log information is stored securely to protect against unauthorized viewing and manipulation.

4.4.5. Audit log backup procedures

All audit log information is stored securely at multiple physically separate locations

4.4.6. Audit Collection System

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by CentralNic personnel and stored using current methods for physical and fire protection.

4.4.7. Vulnerability Assessments

All anomalies in the collected log information are investigated to analyze potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and Compromise Handling Procedures

All actual and suspected events relating to security are defined as incidents. All incidents are handled according to CentralNic's standard procedures.

4.5.2. Corrupted Computing Resources, Software and/or Data

Any defect which would result in the generation of inaccurate data will be caught before publication by the deployment of multiple, independent signing implementations that trigger an incident at any inconsistency.

4.5.3. Entity Private Key Compromise Procedures

A suspected or actual ZSK compromise will be addressed by immediately removing the compromised ZSK from service, replacing it with a newly-generated or pre-generated replacement key. A suspected or actual KSK compromise will be addressed by immediately executing a controlled key rollover.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

CentralNic's organisation-wide business continuity and IT disaster recovery plans include measures to ensure continuity of operation for registry and zone distribution systems including all DNSSEC signing components.

4.6. Entity Termination

If operation of the registry is transferred to another party, CentralNic will participate in the transition so as to make it as smooth as possible according to the same rules and conditions as defined for registrant transfer and cooperation of DNSSEC operations.

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 and specifically authorized personnel in trusted roles. The cryptographic modules are used for the Storage Master Key (SMK), KSK, and ZSK meet the requirements for FIPS-140-2 Level 3 and Common Criteria EAL4+. The SMK, KSK, and ZSK are generated in a key generation ceremony based on proven ceremony implementations as published by IANA and used for the root zone.

5.1.2. Public Key Delivery

One SA, one SO, and one WI must be present throughout the Public Key Delivery process. The public part of each generated KSK pair is exported from the key generation system and verified by the SA and the SO. The SO is responsible for publishing the public part of each generated KSK pair. The SA is responsible for ensuring that the keys that are published are the same as those that were generated. The WI ensures that all processes are followed and any anomalies are documented.

5.1.3. Public Key Parameters Generation and Quality Checking

Key parameters, including the key length and the algorithm type, are verified by the SA, SO and the WI.

5.1.4. Key Usage Purposes

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

5.2. Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed within FIPS-140 certified HSM's and no private keys are ever available in unprotected form outside an HSM.

5.2.1. Cryptographic Module Standards and Controls

For KSK and ZSK key pair generation and signing, CentralNic uses hardware modules that are certified to FIPS 140-2 level 3 and Common Criteria EAL4+.

5.2.2. Private Key (M of N) Multi-Person Control

CentralNic has implemented technical and procedural mechanisms that require participation of a minimum of three out of six trusted individuals to perform sensitive cryptographic operations.

5.2.3. Private Key Escrow

Private components of zone KSK and ZSK are not escrowed.

5.2.4. Private Key Backup

The key archive is encrypted with a Storage Master Key (SMK). The encrypted key archive and SMK are stored on Smart Card in a TL-30 rated safe, only accessible by an SO and Witness.

5.2.5. Private Key Storage on Cryptographic Module

Private keys do not leave the tamper-proof cryptographic module without first being encrypted with the SMK.

5.2.6. Private Key Archival

KSK and ZSK key pairs do not expire, but are retired when superseded.

5.2.7. Private Key Transfer into or from a Cryptographic Module

During the installation of each signing system a shared SMK is transferred via portable media to each HSM. Keys are transferred between HSM's in encrypted key archives stored on portable media.

5.2.8. Method of Activating Private Key

Private keys are activated by putting an HSM on-line. Access to the HSM is provided by an SA; credentials for putting an HSM on-line are held by a SO. Ensuring no process violations occur is provided by the WI.

5.2.9. Method of Deactivating Private Key

Private keys are deactivated by taking an HSM off-line, either by manipulation of the device by an SO or due to a power failure or tamper attempt.

5.2.10. Method of Destroying Private Key

Private keys are not destroyed. After their useful life, keys are removed from the signing system. Tampering with an HSM destroys its contents. If there is any operational issue with an HSM, a controlled tamper will be performed before returning the HSM to the vendor.

5.3. Other Aspects of Key Pair Management

Superseded KSK and ZSK will be never be reused to sign a resource record.

5.4. Activation Data

The activation data are the credentials held by the SO to activate the HSM.

5.4.1. Activation Data Generation and Installation

Each SO is responsible for specifying a PIN, which is used in conjunction with a physical token. The PIN is known only to the SO that specified it. Physical tokens are stored with the HSM they are intended to be used with.

5.4.2. Activation Data Protection

Each SO is responsible for protecting their PIN in a secure fashion. If there is suspicion that a PIN has been compromised, the SO concerned must immediately change it.

5.4.3. Other aspects of activation data

There are no other aspects of activation data.

5.5. Computer Security Controls

All production computer systems are housed in secure facilities. Physical access to computer systems is limited to authorized personnel. Remote (network) access to signing systems is only possible via an authenticated VPN connection by an SA. All attempts to access computer systems, successful and unsuccessful, are logged.

5.6. Network Security Controls

CentralNic's DNSSEC signing infrastructure is logically separated from other components. This separation prevents network access except through defined application processes. CentralNic uses firewalls to protect the DNSSEC signing network from both internal and external intrusion. The network that connects signing systems to HSMs is wholly contained within a locked cabinet that houses the signing systems and HSMs.

All data transfers between signing systems and distribution and validation systems are initiated by the signing system. It is not possible to transfer data to or from a signing system using a transaction initiated from a remote host. Addiionally, firewalls are deployed

5.7. Timestamping

All DNSSEC components are time-synchronised to diverse, reputable time servers using authenticated NTP.

5.8. Life Cycle Technical Controls

All software deployed on production systems can be traced to change management tickets.

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system from the vendors will be applied after formal testing and approval.

Critical hardware components of the signer system (HSM) will be procured directly from the manufacturer and transported in tamper-evidence bags to their destination in the secure facility. All hardware will be decommissioned well before the specified lifetime expectancy.

6. Zone Signing

6.1. Key Lengths and Algorithms

KSK Algorithm: RSASHA256
KSK Length: 2048 bits
ZSK Algorithm: RSASHA256
ZSK Length: 1024 bits

6.2. Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC3 records without OPT-OUT.

6.3. Signature Format

Zone KSK and ZSK signatures are generated using RSA over SHA256 (RSASHA256).

6.4. Key Roll-over

ZSK rollovers are carried out at least every 90 days. ZSKs are pre-published and post-published for at least 7 days,

If a ZSK is believed to be compromised, the ZSK will be published for at most 2 days after the emergency rollover.

KSK rollover is carried out once every year or as revised based on events.

KSKs are pre-published and post-published for at least 30 days.

If a KSK is believed to be compromised, an emergency rollover rollover of the KSK will result in the old key still being published in the one for 7 days.

6.5. Signature Lifetime and Re-Signing Frequency

Resource Record sets (RRSets) are signed with ZSKs with a validity period between six and eight days, using jittered signature lifetime periods and re-signed when the validity period would become less then 6 days

6.6. Verification of Resource Records

Each zone is signed and validated before the signed zone is distributed to name servers using cryptographic software from at least two independent implementations

Orphaned glue records will be removed from the zone prior to signing.

6.7. Resource Records Time-to-Live

The following time-to-live parameters will be used:

SOA: 86400 seconds (24 hours) DNSKEY: 43200 seconds (12 hours) NS, A, AAAA: 86400 seconds (24 hours) RRSIG: inherited from signed RRSet DS: 86400 seconds (24 hours) NSEC3: 3600 seconds (1 hour)

7. Compliance audit

Audits are conducted using stored audit information to ensure system integrity and procedural compliance of all procedures related to the DNSSEC signing system.

7.1. Frequency of entity compliance audit

CentralNic conducts audits at least annually and will conduct more frequent audits in the event of system changes, outages, anomalies or significant staff changes.

7.2. Identity and qualifications of auditor

CentralNic compliance audits are performed by firms that have a well known proficiency in security and DNSSEC.

7.3. Auditor's relationship to audited party

CentralNic will appoint an external auditor who is responsible for the audit's implementation.

7.4. Topics covered by audit

Each audit will include a review of events which occurred during a specified audit period. The auditor will ensure that CentralNic is informed and prepared prior to the audit.

7.5. Actions taken as a result of deficiency

CentralNic will take immediately action to resolve deficiencies found by an audit.

7.6. Communication of results

Results of each audit will be provided to CentralNic in a written report no later than 14 days following the completion of the audit.

8. Legal matters

No fees are charged for any function related to DNSSEC. CentralNic accepts no financial responsibility for security incidents or outages based on its DNSSEC deployments.

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties. Parties must cooperate by removing or adding DS records as requested by the registrant, regardless of standing of the registrant.

This DPS shall be governed by the laws of England and Wales.