DNSSEC Practice Statement for SCB Zone

1. INTRODUCTION

This document, “DNSSEC Practice Statement for SCB Zone” (DPS) states the practices and provisions that Thai Name Server Co., Ltd. (TNS) employs in providing DNSSEC for SCB zone.

1.1. Overview

DNSSEC (Domain Name System Security Extensions) is a set of IETF specifications for enabling origin authentication and data integrity verification of the DNS data. This is done by incorporating public key cryptography into the DNS hierarchy to form a chain of trust. The fundamental specifications of DNSSEC are described in following RFCs: 4033, 4034 and 4035.

This DPS is a document states the practices and procedures of TNS with regard to DNSSEC operations for SCB zone. This document conforms to A Framework for DNSSEC Policies and DNSSEC Practice Statements (RFC 6841), (http://tools.ietf.org/html/rfc6841).

1.2. Document name and identification

Document title:	DNSSEC Practice Statement for SCB Zone
Version:	1.0
Available date:	26 May 2014
Effective date:	01 July 2014

1.3. Community and Applicability

1.3.1. Registry

Thai Name Server Co., Ltd. is the Back-end Registry Operator (Registry) for the SCB zone. It is the responsibility of the Registry to:

- Generate signing keys, Key Signing Key (KSK) and Zone Signing Key (ZSK)
- Sign the SCB zone
- Submit DS records of containing the KSK public key to IANA for insertion into the root zone
- Receive DS Resource Records from Registrar and update the zone accordingly

1.3.2. Registrar

The Registrar of SCB is an ICANN Accredited Registrar who enables registrants to submit the DS records of their zones to the Registry.

1.3.3. Registrant

The Registrant, Child zone manager, is an entity who registers in, and operates on the delegated domain, and as such is responsible for:

- Generating the keys associated with the zone

- Signing their zone
- Registering and maintaining the shorthand representations of KSK public keys of its zones, in the form of Delegation Signer (DS) Resource Records, in the SCB zone through the Registrar

1.3.4. Relying party

Relying parties are all the entities related to the SCB DNSSEC Service, including caching DNS server operators and users who utilize their services.

1.3.5. Applicability

The DPS is applied to the zone of the TLD SCB. Delegated child zones are outside the scope of this DPS.

1.4. Specification Administration

1.4.1. Specification administration organization

Thai Name Server Co., Ltd.

1.4.2. Contact information

DPS Coordinator
Thai Name Server Co., Ltd.
159 Phichai Road
Thanonnakornchaisri, Dusit
Bangkok, Thailand
10300
Telephone: +66-2-105-4291 (09:00 – 17:00 UTC+7, excluding Saturdays, Sundays, Thai public holidays)
E-mail: dps_scb@thains.co.th

1.4.3. Specification change procedures

The Registry reviews and revises this DPS periodically and/or in case of arising legitimate needs. After approval of changes by the General Manager of the Registry, the updated DPS will be effective immediately upon publication.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

Information on the DPS will be published on the Registry's web site at www.thains.co.th/docs/scb/dnssec/

The DPS on the web site is publicly accessible with read-only access.

2.2. Publication of public keys

The Registry publishes the SCB KSK public key as DNSKEY in the SCB zone. The DS records for the SCB KSK public key will be published in the root zone. The Registry does not explicitly publish the KSK public key of the SCB zone as a trust anchor and recommends against its use for that purpose.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of Domain Names

DNSSEC provides mechanisms for ensuring that the DNS data delivered to clients is consistent with the information in the registry. It does not provide any way of determining the purpose and meaning of the domain names.

3.2. Identification and Authentication of Child Zone Manager

The identity and authority of the Child Zone Manager will be conducted by the SCB Registrar. The Registry applies changes received from the Registrar.

3.3. Registration of Delegation Signer (DS) Resource Records

The DS records can be submitted by the Child Zone Manager to the Registry through the Registrar. Upon the request from Registrar, the Registry registers DS Resource Record(s) into the SCB zone. Up to eight DS records can be registered per child domain.

3.4. Method to Prove Possession of Private Key

The Registry does not specify requirements of validation made by Registrar to prove possession of private key of KSK corresponding to the DS record in the request.

3.5. Removal of DS Resource Records

The removal of DS Resource Records can be requested by the Child Zone manager through the Registrar. Upon the request from Registrar, the Registry removes the DS records from the SCB zone.

4. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

The Registry DNSSEC service is conducted within a protected facility that prevents unauthorized access to sensitive information and the systems. The Registry also maintains secondary facilities for its DNSSEC service.

4.1.2. Physical access

All facilities have restricted access, limited to authorized personnel

4.1.3. Power and Air conditioning

The facilities are equipped with highly efficient power backup system and redundant air cooling system.

4.1.4. Water exposure

The registry takes reasonable precautions to minimize the impact of water exposure to the Registry systems.

4.1.5. Fire prevention and protection

All facilities have fire detection systems.

4.1.6. Media storage

The Registry stores media containing important data and backup in an environment that limits access to authorized personnel.

4.1.7. Waste disposal

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

4.1.8. Off-site backup

The Registry stores the specified important backup information and audit logs related to DNSSEC service in a physically secure manner at the Registry's office separate from the DNSSEC operation facilities.

4.2. Procedural Controls

4.2.1. Trusted roles

Trusted roles are held by individuals that are involved in the generation or use of private key material, delivery and publication of public keys. The trusted roles are:

- Systems Administrator, SA
- Security Officer, SO

A single individual may not hold more than one trusted role at a time. No individual may undertake any trusted role within 7 days of relinquishing a different role.

The Registry considers the categories of personnel identified in this section as Trusted Persons having a Trusted Role. Persons seeking to become Trusted Persons by obtaining a Trusted Role must successfully complete the screening requirements set out in this DPS.

4.2.2. Number of persons required per task

Separation of duties and roles is enforced for critical operations.

For each DNSSEC key ceremony at least 2 System Administrators, 4 Security Officers are physically required to be present.

For the others task, at least 1 System Administrator and 1 Security Officer are required.

4.2.3. Identification and authentication for each role

Verification of identity is performed through a check of the Registry issued identification. Permissions to operate the DNSSEC related facilities are authenticated and authorized for each trusted person, and recorded with their identification.

4.2.4. Tasks requiring separation of duties

All tasks requiring separation of duties include, but not limited to, generation, activation or destruction of DNSSEC key materials.

The trusted roles in 4.2.1 above may not be held simultaneously by one and the same person. The separation of duties is forced by the Security Officer not having exclusive physical access to the operational facilities, and the System Administrator not having access to the activation material of the Hardware Security Module (HSM).

4.3. Personnel controls

4.3.1. Qualifications, experience, and clearance requirements

The Registry requires that employees seeking to become Trusted Persons are limited to full time employees of the Registry or those who are specifically approved by the Registry.

4.3.2. Background check procedures

Background checks are performed as part of the hiring process for all personnel

4.3.3. Training requirements

The Registry periodically reviews and enhances training programs as necessary.

4.3.4. Job rotation frequency and sequence

Not applicable in this document.

4.3.5. Sanctions for unauthorized actions

Disciplinary actions will be undertaken for unauthorized actions with respect to this DPS and/or other violations of the policies and procedures. Disciplinary actions may include:

- Measures up to and including termination
- Liability of damages
- Prosecution.

Disciplinary action will be assessed with regard to the frequency and severity of the unauthorized actions.

4.3.6. Contracting personnel requirements

Only personnel in specified trusted roles are permitted access to the SCB DNSSEC systems. If needed, an authorized team member can perform tasks with the guidance of an external contractor. At no time, however, are external contractors or third parties permitted access to perform tasks directly on these systems.

4.3.7. Documentation supplied to personnel

The Registry provides personnel training and required documents needed to perform their job responsibilities for the SCB DNSSEC service.

4.4. Audit logging procedures

4.4.1. Types of events recorded

The Registry manually or automatically logs the following events:

- Key generation, backup, storage, recovery, and destruction
- Key activation
- Zone change events
- Key rollover events
- Security-related events, including:
    - Successful and unsuccessful system access attempts
    - System crashes and hardware failures
    - System changes and maintenance/system updates

The record of events includes date and time of each event, the entity that initiated the event and the contents of the event.

4.4.2. Frequency of processing log

The Registry checks the audit logs at a frequency sufficient to monitor for suspicious or unusual activity within the Registry zone signing systems. If any suspicious activity is detected, immediate notification will be made to appropriate personnel.

4.4.3. Retention period for audit log information

The Registry keeps the audit logs for at least 90 days in a manner of being able to access them promptly. Archives of the audit logs are kept for at least 1 year.

4.4.4. Protection of audit log

These logs are not available to unauthorized employees and cannot be modified.

4.4.5. Audit log backup procedures

The Registry backups the audit logs periodically. This media is stored in a physically secure manner.

4.4.6. Audit collection system

A log collection system records DNSSEC service activities at the application and operating system level. Manually generated audit logs are recorded by the Trusted Persons and stored in secure storage.

4.4.7. Vulnerability assessments

The audit log information is investigated and analyzed for potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

The incident handling procedures includes conducting a root-cause analysis, to formally identify the nature and impact of the event and to identify what measures is required to prevent the event from reoccurring (or to limit its consequences). The procedures also include the escalation and reporting of incidents to the appropriate authority within the Registry.

4.5.2. Corrupted computing resources, software, and/or data

In the event of the corruption of computing resources, and/or data, the Registry attempts to recover by using backup hardware, software or data according to the prescribed recovery plan.

4.5.3. Entity private key compromise procedures

If a zone signing key (ZSK) is suspected of having been compromised, the Registry will immediately stop using that key, and, if necessary, a new ZSK will be generated. The old key will be removed from the key set as soon as its signatures have expired or timed out, or with certainty been discarded from the resolvers, whichever occurs first. If a ZSK is suspected of having been completely compromised and revealed to unauthorized parties, this will be notified through the appropriate channels.

If a key signing key (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 the key set until it can be considered sufficiently safe to remove the key, taking into account the risk for disruptions in relation to the risk presented by the compromised key. A KSK rollover is always announced through the channels.

If the KSKs (and possibly also the ZSKs) are lost completely, new keys will be generated at the earliest possible occasion and included in the key set. In the meantime it can occur that the .SCB zone will remain unsigned until the system has been restored and new DS records been published in the root zone. Any scheduled ZSK rollovers during this time will be postponed.

4.5.4. Business continuity and IT disaster recovery capabilities

The Registry has developed a business continuity and IT disaster recovery plan to mitigate the effects of natural, man-made or technological disasters that require temporary or

permanent cessation of operations from any of the Registry's facilities. The business continuity and IT disaster recovery plans are in place to address the restoration of information systems services and key business functions.

4.6. Entity termination

The Registry has implemented a DNSSEC termination plan in case of transition to a new registry. The Registry will co-ordinate with the successor registry in order to execute the transition in a secure and transparent manner.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Key pair generation, (KSK and ZSK), takes place in an HSM that is managed by authorized personnel in the trusted roles (SA and SO).

All keys for the SCB zone are normally generated at a formal key ceremony. The generation of the keying material includes KSK, ZSK and others used for access control, key distribution and backup. In case of an Emergency that requires new keys, they may be generated by authorized persons assigned by Management.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the Security Officer and System Administrator. The Security Officer is responsible for publishing the public component of the KSK as per 2.2. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Public key parameters generation and quality checking

The key parameters are defined by the Registry DPS committee. The control includes checking the key length during key generation.

5.1.4. Key usage purposes

The SCB zone KSK and ZSK private keys will be used only for signing the SCB zone.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed within the HSMs.

5.2.1. Cryptographic module standards and controls

The HSM is FIPS 140-2 level 3 certified. Access to the HSM is specified in Section 4.2 and 4.3.

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

The Registry does not enforce multi-person control for private key operations. Refer to section 4.2.4 for compensating controls through separation of duties in the HSM Activation Process.

5.2.3. Private Key escrow

Private keys of SCB KSK & ZSK are not escrowed.

5.2.4. Private Key backup

Immediately after the key generation, the KSKs and ZSKs are copied to an HSM backup module. The HSM backup module and the token are stored in the secure storage at the Off-site backup described in section 4.1.8. Backup process is performed according to the prescribed backup plan.

5.2.5. Private Key storage on cryptographic module

Private keys are stored on HSM in encrypted form.

5.2.6. Private Key archival

The private keys which are no longer use are not archived.

5.2.7. Private Key transfer into or from a cryptographic module

The backup process requires the private key to be transferred. When private keys are generated on the main HSM, they will be transferred to an HSM backup module. After that the keys will be transferred from the HSM backup module to the other HSM in an encrypted form.

5.2.8. Method of activating private key

The private key will be activated by a system administrator and a security officer. The administrator has to activate the partition on the HSM using password, token and PIN. Then the signing machine is able to access the partition on the HSM using partition password. Once the partition is activated, the key is active for an indefinite period.

5.2.9. Method of deactivating private key

The private key will be deactivated by a system administrator and security officer. The administrator has to deactivate the partition on the HSM using password, token and PIN.

5.2.10. Method of destroying private key

The private key on the HSM can be deleted by a system administrator and a security officer using password, token and PIN.

5.3. Other aspects of key pair management

Keys will be ceased when their production utilization ends. The keys will not be reused and archived.

5.4. Activation data

5.4.1. Activation data generation and installation

Activation data is generated mechanically, and stored in a token used to activate the HSM. The installation of the activation data is made by coupling the HSM to the token.

5.4.2. Activation data protection

Each Security Officer is responsible for protecting the activation data and tokens according to the Registry rules. While the tokens are not in use, they are stored in safes that are only accessible by authorized persons.

5.4.3. Other aspects of activation data

In the event of an emergency, there exists another set of activation data in a sealed, tamper evident package at a secure location. That activation data can be used. The Registry business continuity plan states the conditions in which this procedure shall be enacted.

5.5. Computer Security Controls

Only authorized computers are allowed to use. All critical operations related to the DNSSEC service will be logged and traceable. All personnel with access to these systems must use individual access credentials. No-one is permitted to borrow the credentials of another, not to reveal their credentials to anyone, other than as required by law.

5.6. Network Security Controls

Firewalls are applied to networks, and access from outside of the networks is limited to minimum necessary for the operation of the system. The registry systems are splited into a number of different VLANs, security zones and filtered by the firewalls.

5.7. Timestamping

The Registry synchronizes all system clocks using the Network Time Protocols. An external stratum one NTP server, within Thailand if possible, such as at the National Institute of Metrology (Thailand), is used to provide the reference time.

5.8. Life cycle technical controls

The registry system is developed in-house as a part of the Registry’s work with version control. Any new versions are tested in a test environment. Only when all tests are completed and successful, they can be rolled out to production environments. A security audit will be performed at regular intervals.

6. ZONE SIGNING

6.1. Key Lengths, Key Types, and Algorithms

The key length of the KSK is 2048 bits and 1024 bits for the ZSK. The algorithm for both KSK and ZSK is RSASHA256.

6.2. Authenticated denial of existence

The Registry uses NSEC3 with Opt-OUT as defined in RFC 5155.

6.3. Signature format

The digital signature algorithm used to sign the TLD zone file is RSA/ SHA-2 as defined in RFC 5702.

6.4. Key rollover

Zone signing key (ZSK) rollover is carried out every 90 days.
Key signing key (KSK) rollover is carried out as required.

6.5. Signature lifetime and re-signing frequency

RR sets are signed with ZSKs with a validity period of fourteen days and are resigned every 2 days.

6.6. Verification of resource records

The registry verifies that all resource records are valid in accordance with the current standards prior to distribution.

6.7. Resource records time-to-live

RRtype	**TTL**
DNSKey	2 hours
Delegation Signer (DS)	2 hours
NSEC3	1 hour
RRSIG	same as the covered RR except for NSEC3 related

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

Compliance audits are conducted annually.

7.2. Identity/qualifications of auditor

Auditor should have at least two-year experience in conducting IT security audits; possess knowledge of IT security standard and the DNSSEC protocol.

7.3. Auditor's relationship to audited party

Each compliance audit is performed by an auditor that is independent of The Registry.

7.4. Topics covered by audit

Topics cover DNSSEC described in DPS.

7.5. Actions taken as a result of deficiency

Any deficiency identified during a compliance audit will be reported to the Registry. The Registry will apply operational improvements as necessary.

7.6. Communication of results

The results of the audit shall be submitted as a written report to the Registry within 60 days following the completion of the audit. The auditing reports are not made public.

8. LEGAL MATTERS

The Registry has no legal responsibilities for the matters described in the SCB DPS. The Registry operates the DNSSEC Service in accordance with and governed by the laws of Thailand.