DNSSEC Practice Statement (DPS)

1. INTRODUCTION

This document, "DNSSEC Practice Statement for the ".TOP" zone (".TOP" DPS)"， states ideas of policies and practices of KNET with regard to DNSSEC operations for the ".TOP" zone.

1.1. Overview

KNET has published ".TOP" DPS to provide operational information about DNSSEC for the ".TOP" zone. To accomplish comprehensive investigation into the ideas of operational security, policies, practices and procedures of DNSSEC service for the ".TOP" zone ("KNET DNSSEC Service"), ".TOP" DPS adopts the DPS framework which is proposed and discussed in IETF Domain Name System Operations (DNSOP) Working Group.

Chapters of this document are shown as follows.

1.2. Document Name and Identification

DNSSEC Practice Statement for the ".TOP" zone (".TOP" DPS)
Version: 1.1
Available on: 2011/11/23
Effective on: 2011/12/23

1.3. Community and Applicability

In this section, associated entities and their roles regarding KNET DNSSEC Service are described.

1.3.1. Registry

JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. is the Registry for the ".TOP" domain names. KNET as DNS service provider, administrates registrations of domain names and operates DNS servers for the ".TOP" zone. As for KNET DNSSEC Service, the KNET generates signing keys (KSK and ZSK) of the ".TOP" zone and signatures for the ".TOP" zone. Further, through registering DS record(s) of the Registry into the root zone, the Registry enables origin authentication and data integrity verification of records in the ".TOP" zone by using KSK of the root zone as a trust anchor.

1.3.2. Registrar

JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. Registrar of the “.TOP” domain names is an entity who has concluded an agreement with the JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. for agency operations on “.TOP” domain name registrations. JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. Registrar submits various requests regarding registrations of domain name information, including DS records in the “.TOP” zone.

1.3.3. Registrant

Registrant is an entity who has registered “.TOP” domain name(s) info the Registry. For deploying DNSSEC into the Registrant's domain name(s), Registrant generates signing keys and composes digital signatures on Registrant's zone ("Registrant Zone"). Registrant enables origin authentication and data integrity verification of Registrant Zone by registering DS record(s) into the Registry through Registrar.

1.3.4. Relying party
Relying party is all the entities related to DNSSEC Service, including recursive DNS server operators and users who utilize their services.

1.4. Specification Administration

1.4.1. Specification administration organization

Co., Ltd. (KNET)

1.4.2. Contact information

Contact: Lu Wenzhe
Email: lwz@knet.cn
Phone: 86-10-58813017

1.4.3. Specification change procedures

KNET may amend the DPS without notification for changes that are not considered significant. All changes to this DPS will be approved by the JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. and be effective immediately upon publication.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

“.TOP” DPS (Chinese)
http://www.zdns.cn/doc/top-dps-cn.html

“.TOP” DPS (English)
http://www.zdns.cn/doc/top-dps-en.html

2.2. Publication of Key Signing Keys

KNET composes a chain of trust of DNSSEC by registering a DS record of the “.TOP” zone into the root zone. Therefore, the Registry does not explicitly publish KSK public key of the “.TOP” zone as a trust anchor.

2.3. Access Controls on Repositories

The Registry does not perform particular access controls on “.TOP” DPS except for read only access.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of Domain Names

The purpose and meaning of registration of domain names in the “.TOP” zone follows descriptions in documents below. (Political restriction)

3.2. Activation of DNSSEC for Registrant Zone

When a DS record corresponding to a signing key used in a given Registrant zone is published in the “.TOP” zone, which is operated by KNET, and digitally signed with a signing key of the “.TOP” zone, a chain of trust from the “.TOP” zone to the Registrant Zone comes to be composed. This enables the Registrant zone to be activated as a DNSSEC-aware zone.

3.3. Identification and Authentication of Registrant Zone Manager

JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. does not conduct any identification or authentication of the child zone manager as it only applied changed received from Registrar of Record.

3.4. Registration of Delegation Signer (DS) Records

The submission of a DS record is carried out by the Registrar of Record using the SRS interface (EPP) into the registry system.

3.5 Method to Prove Possession of Private Key

Since the DS record submitted by Registrant will be validated based on the KSK record in the child zone, the child zone manager is not required to provide proof of the possession of the private component of KSK in the child zone.

3.6. Removal of DS Record

3.6.1. Who can request removal

The Registry removes DS records for the Registrant Zones from the ".TOP" zone based on the requests from Associated Registrars. Associated Registrars confirm the intentions of removal with the Registrants before requesting removals.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

KNET operations are conducted within a physically protected room, which prevents unauthorized access. The room is not easily affected by disasters including water exposures, earthquakes, fires and thunder strikes. KNET also prepares backup facility to meet the minimum standards applied to the normal facility in terms of physical security, power supper, environment and earthquake, fire and water protection. The redundant facility contains a complete set of the KNET's critical systems, whose information will be automatically synchronized with normal operation facility.

4.1.2. Physical access

Only authorized personnel have the physical access right. And the entry will be logged and the environment is continuously monitored.

4.1.3. Power and air conditioning

Power is provided to the operation facilities through at least two separate sources. In case of power outages, UPS will provide power until the backup power system works.

4.1.4. Water exposures and earthquakes

Flooding protection and detection mechanisms are implemented by the facilities

4.1.5. Fire prevention and protection

The facilities are equipped with fire detection and extinguishing systems.

4.1.6. Media storage

The Registry stores recording media containing important archive/backup data related to KNET DNSSEC Service in storage cabinet(s) within a room where entry and exit are controlled appropriately.

4.1.7. Waste disposal

KNET will dispose storage media and other material that may contain sensitive information in a secure manner.

4.1.8. Off-site backup

Critical data related to DNSSEC Service is securely stored using a storage facility. The facility is separated from KNET's other facilities and only authorized personnel have the access right.

4.2. Procedural Controls

4.2.1. Trusted role

Trusted roles are in charge of maintaining the zone file and key rolling.

1. Systems administrator (SA)
2. Security Officer (SO)

4.2.2. Number of persons required per task

For zone data modification, key rolling event, at least one SA and one SO should be present.

4.2.3. Identification and authentication for each role

Only people who have worked in KNET for at least 3 years and accept DNSSEC related training are granted to hold a trusted role. All the trust roles have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with KNET.

4.2.4. Tasks requiring separation of duties

All the DNSSEC related operation can’t be performed by only one person. And none of the trust roles can be held simultaneously by one person.

The ZSK rolling, KSK rolling, and zone maintaining will be assigned to different person.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Persons who have "Trusted Role" as described in 4.2.1 are limited to employees of KNET for at least 3 years.

4.3.2. Background check procedures

The following items will be reviewed:

- The candidates resume,
- Previous employments
- Documentation confirming relevant education experience
- Financial position through a credit check.

4.3.3. Training requirements

The Registry gives trainings to personnel in charge of KNET DNSSEC Service as follows:

- Before having roles of operating KNET DNSSEC Service, required trainings for the roles are performed.
- When operational procedure is changed, affected descriptions in operation manuals are updated promptly and trainings associated with the change are provided.

4.3.4. Re-training frequency and requirements

The Registry periodically examines the necessity of re-training for personnel in charge of KNET DNSSEC Service. Re-training is provided as necessary.

4.3.5. Job rotation frequency and sequence

Personnel are rotated and replaced as needed.

4.3.6. Sanction for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions with respect to this DPS.

4.3.7. Contracting personnel requirements

Not applicable in this document.

4.3.8. Documentation supplied to personnel

Necessary documentation will be provided to related person to perform their work task in a secure and related easy manner.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

In order for detecting incorrect/illegal operations and proving legitimacy of operations related to KNET DNSSEC Service, the Registry records following events as "the Audit Logs":

- Events of access to facilities for KNET DNSSEC Service
- Events of operations using signing keys
  + Activation of KSK used for KNET DNSSEC Service
  + Generation/Deletion of KSK/ZSK used for KNET DNSSEC Service
  + Roll-over of KSK/ZSK used for KNET DNSSEC Service
  + Composition of signature for the “.TOP” zone by KSK/ZSK
  + Registration of DS record(s) of the “.TOP” zone into the root zone
- Events of confirmation for recorded facts in the Audit Logs

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

4.4.2. Frequency of processing log

Logs are analyzed each day. Specific controls are conducted on processes including key rolling, system reboots and detected anomalies.

4.4.3. Retention period for audit log information

Log information is stored for 1 month. Archives of the Audit Logs are kept for at least 3 years.

4.4.4. Protection of audit log

The Registry limits access to the Audit Logs to only necessary personnel in order to protect the Audit Logs from browse, modification or deletion by unauthorized parties.

4.4.5. Audit log backup procedures

The Registry backups the Audit Logs on external media storage periodically. This media is stored in lockable cabinet(s) in a room where entry and exit are controlled appropriately.

4.4.6. Audit collection system

Offline Audit Logs are recorded by the Trusted Roles and stored in secure storage cabinet(s) at facility managed by KNET.

4.4.7. Notification to event-causing subject

Not applicable in this document.

4.4.8. Vulnerability assessments

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

4.4. Compromise and Disaster Recovery

4.4.1. Incident and compromise handling procedures

If the private key of the ".TOP" zone is (likely to be) compromised, the Registry carries out emergency roll-over of the signing key. When KNET DNSSEC Service becomes discontinued due to accidents or disasters, the Registry attempts to restart KNET DNSSEC Service as quickly as possible.

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

When important hardware, software or data related to KNET DNSSEC Service is broken or damaged, the Registry will attempt to recover it promptly using backup hardware, software or data according to the prescribed recovery plan.

4.4.3. Entity private key compromise procedures

When the KSK of the ".TOP" zone becomes compromised, the Registry carries out the following procedures:

- Re-generation of KSK of the ".TOP" zone and put into use ASAP.
- Old key will remain in place and be used to sign key sets
- New DS record will be send to root zone to replace old DS
- After Sufficient time (KSK TTL + key transfer time + DS replaced in root zone) elapsed, old key and the signature generated by it will be removed from ".TOP" zone.

When the ZSK of the ".TOP" zone becomes compromised, the Registry carries out the following procedures:

- Re-generation of ZSK of the ".TOP" zone;
- Composition of signature for DNSKEY records containing re-generated ZSK by KSK of the ".TOP" zone; and
- Composition of signatures for authoritative records in the KNET zone by re-generated ZSK.

- Old key will be removed after sufficient time (max TTL of record in ".TOP" zone + key transfer time)

In case of KSK emergency rolling, all the relying parties will be notified to refresh their static configuration to add the emergency KSK as extra trust-anchor.

4.4.4. Business continuity and IT disaster recovery capabilities

For cases where continuation of KNET DNSSEC Service is disabled due to damage on the facilities by a disaster, the Registry attempts to recover the service shortly on the remote backup-site configured beforehand.

4.5. Entity Termination

If the KNET must stop DNSSEC service for host zones for any reason, defined procedures will be followed and general public will be informed. If operations are transferred to another party, KNET will corporate with them to make it as smooth as possible.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Hardware security module (HSM) is used to generate KNET keys, including ZSK and KSK. Key generation must be performed by two people working in unison. The entire procedure is logged.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by SO and SA. The SO is in charge of publishing the public components of KSK and the SA makes sure that the key is same with that are generated.

5.1.3. Public key parameters generation and quality checking

The Registry periodically confirms that generation of signing key is conducted with appropriate parameters in the context of technological trends.

5.1.4. Key usage purposes

The Registry uses the signing keys only for generating signatures for the ".TOP" zone and does not use them for any other purposes.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic module standards and controls

The system uses a HSM which conforms to the requirements in FIPS 142-2 level 3.

5.2.2. Private key multi-person control

A SO is required to active the HSM, and for physical access to HSM, A SA is required.

5.2.3. Private key escrow
Private keys of the “.TOP” zone are not escrowed.

5.2.4. Private key backup
After key generation it will be securely backed up into another HSM.

5.2.5. Private key storage on cryptographic module
Private key will be stored in several HSM.

5.2.6. Private key archival
Obsolete private keys are not archived, except for backups mentioned above.

5.2.7. Private key transfer into or from a cryptographic module
HSM will prevent export private keys. Keys can only be transferred using portable USB media between HSM and the key info is encrypted.

5.2.8. Method of activating private key
An SA provides an SO with access to HSM, the SO states a personal passphrase for the HSM through a console.

5.2.9. Method of deactivating private key
Once the signing system isn't active, the HSM will lock the private Key.

5.2.10. Method of destroying private key
When keys are not used by the signing system, they are removed from the HSM.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival
Public keys are archived in the same way like log data.

5.3.2. Key usage periods
The upper limit of usage period for KSK is one year plus appropriate period for transition. The upper limit of usage period for ZSK is one month. The Registry may change these periods as necessary.

5.4. Activation Data

5.4.1. Activation data generation and installation
Each SO is responsible for creating their own activation data which should consist of 9 characters of varying nature.

5.4.2. Activation data protection

SO protects activation data in a sufficiently secure manner. On the suspicion of compromised activation data, the SO must immediately change it.

5.4.3. Other aspects of activation data

In order to prepare for emergencies, SO seals a copy of activation data in envelope(s) with tamper trail. In case of arising necessity to break this seal, it will be done under control of an Emergency Security Officer (ESO).

5.5. Computer Security Controls

On the important components of KNET DNSSEC Service System ("the Important Components"), only minimum necessary software defined by the Registry runs. All the important operations on the Important Components will be logged. All the authentication credentials used to access the Important Components are properly controlled. The Important Components are monitored continuously, and if any abnormalities or illegal operations on them are detected, the Registry takes appropriate countermeasures promptly.

5.6. Network Security Controls

Firewalls are applied to networks on which KNET DNSSEC Service is deployed, and access from outside of the networks is limited to minimum necessary protocols defined by the Registry.

5.7. Timestamping

The Registry obtains time for KNET DNSSEC Service System from reliable time source(s) and synchronizes the system clocks with it. As for KNET DNSSEC Service System, the Registry obtains time from NTP (Network Time Protocol) and synchronizes the system clocks. The synchronized times are used for time stamping for the audit logs and inception/expiration time for validity period of RRSIG.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

The Registry controls each process at system development and evaluates the system prior to deploying it, in order to maintain the quality and security of KNET DNSSEC Service System.

5.8.2. Security management controls

As security controls of KNET DNSSEC Service System, the registry undertakes counter-measures such as entering/leaving controls, staff controls including training, operation controls including authority control and system controls including intrusion protection and virus protection.

5.8.3. Life cycle security controls

The Registry evaluates periodically whether the development of KNET DNSSEC Service System is controlled under prescribed manner. Moreover, the Registry gathers information related to security, surveys technical trends, and evaluates/improves the system as necessary.

6. ZONE SIGNING

6.1. Key Length and Algorithms

Algorithms defined by the protocol standards are adopted for signing keys of the ".TOP" zone. Algorithm and key length for signing key that are considered secure for the usage period are adopted. Therefore, the algorithm for both KSK and ZSK is RSA/SHA1, and the key length of KSK is 2048 bits and that of ZSK is 1024 bits.

6.2. Authenticated Denial of Existence

For authenticated denial of existence in the ".TOP" zone, the method using NSEC3 records with Opt-Out flag specified in RFC 5155 is adopted. The values of hash algorithm, iterations and salt are set to SHA-1, random number around ten times and random string of approximately ten hexadecimal characters, respectively.

6.3. Signature Format

The signature format for records in the ".TOP" zone is RSA/SHA-1 specified in RFC 3110.

6.4. Zone Signing Key Roll-over

In the ".TOP" zone, roll-over of ZSK is carried out on a monthly basis by the pre-publish method described in RFC 4641.

6.5. Key Signing Key Roll-over

In the ".TOP" zone, roll-over of KSK is carried out on an annual basis by the double signature method described in RFC 4641.

6.6. Signature Validity Period and Re-signing Frequency

In the ".TOP" zone, signature validity period for KSK is around 2 months, while that for ZSK is around 1 month. Re-signing frequencies for KSK and ZSK are per month and per week, respectively.

6.7. Verification of Zone Signing Key Set

Before pre-publishing of ZSK, the Registry checks that each of following processes is performed correctly:

- Generation of ZSK by HSM;
- Addition of the ZSK to DNSKEY RRset and composition of signature to the RRset with KSK ;
- Transmission of the ZSK and signature for the RRset to KNET DNSSEC Service System using dedicated secure channel(s); and

- Verification of whether the ZSK composes chain of trust to the “.TOP” zone.

6.8. Verification of Resource Records

The Registry verifies that all the Resource Records are compliant with the protocol standards before they are published on the “.TOP” zone.

6.9. Resource Records TTL

In the “.TOP” zone, TTL of DNSKEY, DS and their corresponding RRSIG is set to 86400 (1 day). TTL of NSEC3 and the corresponding RRSIG is set to 900 (15min.), which is the same as negative cache value for the “.TOP” zone. Those TTLs may be changed into appropriate values along with technical trends.

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

Compliance audits are conducted at least annually. Additional audits will be carried out including the following circumstances:

Recurring discrepancies or incidents

Significant changes at the management, organizational or process level

7.2. Identity/qualifications of auditor

The auditor shall be able to demonstrate proficiency in information security auditing, IT security, DNS and DNSSEC.

7.3. Auditor’s relationship to audited party

KNET will appoint an independent third-party auditor who is responsible for the audit’s implementation.

7.4. Topics covered by audit

The scope of JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD.'s annual compliance audit includes all DNSSEC operations such as key environmental controls, key management operations.

7.5. Actions taken as a result of deficiency

Any deficiencies discovered during the audit will be communicated to the top management of JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD.. The severity of each discrepancy will be determined with input from the auditor, and an appropriate correction plan will be developed and implemented.

7.6. Communication of results

The results of the audit shall be submitted as a written report to JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. within 30 days following the completion of the audit. The audit reports are not made public.

8. LEGAL MATTERS

8.1. Fees
No fees are charged for any function related to DNSSEC.
8.2. Financial Responsibility

JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. accepts no financial responsibility for improper use of Trust anchors or signatures, or any other improper use under this DPS.
8.3. Confidentiality of business information
8.3.1. Scope of confidential information

The following information shall be kept confidential and private:
Private keys and information needed to recover such Private Keys
Audit logs
Reports created by auditor
Security measures controlling the operations of JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. hardware and software

8.3.2. Types of information not considered confidential
Information that is classified as public as part of the DNSSEC extensions to DNS are considered to be public by JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. and will not be subject to access restriction.

8.3.3. Responsibility to protect confidential information
JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. secures confidential information against compromise and disclosure to third parties.

8.4. Privacy of personal information

8.4.1. Information treated as private
Not applicable.

8.4.2. Information not deemed private
Not applicable.

8.4.3. Responsibility to protect private information
Not applicable.

8.4.4. Disclosure Pursuant to Judicial or Administrative Process
JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. shall be entitled to disclose Confidential/Private Information if, in good faith, JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. believes that disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for

production of documents.

8.5. Limitations of liability

JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. shall not be liable for any financial loss or loss arising from incidental damage or impairment resulting from its performance of its obligations hereunder or the Registry Operator's or obligations under DNSSEC Practice Statement. No other liability, implicit or explicit, is accepted.

8.6. Term and termination

8.6.1. Term

The DPS becomes effective upon publication in the JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. repository. Amendments to this DPS become effective upon publication in the JIANGSU BANGNING SCIENCE & TECHNOLOGY CO.,LTD. repository.

8.6.2. Termination

This DPS as amended from time to time and will remain in force until it is replaced by a new version.

8.6.3. Dispute resolution provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

8.6.4. Governing law

This DPS shall be governed by the laws of the People's Republic of China.