DNSSEC Policy and Practice Statement for ".CN" Zone

CNNIC

Document Control

SECURITY CALSSIFICATION	File Name
Public	DNSSEC Policy and Practice Statement for ".CN" Zone

Audits

Date	Version	Update	Description
2013-07-18	Version-1.0	DNSSEC Workgroup	First Version

Table of Contents

DNSSEC Policy and Practice Statement for ".CN" Zone 1
Document Control 2
Audits 2
Table of Contents 3
1 Introduction 1
1.1 Overview 1
1.2 Document Name and Identification 1
1.3 Community and Applicability 1
1.3.1 Registry 2
1.3.2 Registrar 2
1.3.3 Registrant 2
1.3.4 Relying Party 2
1.3.5 Applicability 3
1.4 Specification Administration 3
1.4.1 Specification Administration Organization 3
1.4.2 Contact Information 3
1.4.3 Specification Change Procedures 3
2 Publication and Repositories 4
2.1 Publication site 4
2.2 Publication of Key Signing Keys (KSK) 4
2.3 Access Controls on Repositories 4
3 Operational Requirements 4
3.1 Meaning of Domain Names 4
3.2 Activation of DNSSEC for Child Zone 5
3.3 Identification and Authentication of Child Zone Manager 5
3.4 Registration of Delegation Signer (DS) Resource Records 5
3.5 Method to Prove Possession of Private Key 5
3.6 Removal of DS Resource Records 6
4 Management, Operational and Physical Control 6
4.1 Physical Controls 6
4.1.1 Site Location and Construction 6
4.1.2 Physical Access 6
4.1.3 Power and Air Conditioning 6
4.1.4 Water Exposures 7
4.1.5 Fire Prevention and Protection 7
4.1.6 Media Storage 7
4.1.7 Waste Disposal 7
4.1.8 Off-site Backup 7
4.2 Procedural Controls 8
4.2.1 Trusted Roles 8
4.2.2 Number of Persons Required Per Task 8

4.2.3 Identification and Authentication for Each Role 8
4.2.4 Tasks Requiring Separation of Duties 9
4.3 Personnel Controls 9
4.3.1 Qualifications, Experience, and Clearance Requirements 9
4.3.2 Background Check Procedures 9
4.3.3 Training Requirements 9
4.3.4 Retraining Frequency and Requirements 10
4.3.5 Job Rotation Frequency and Sequence 10
4.3.6 Sanctions for Unauthorized Actions 10
4.3.7 Contracting Personnel Requirements 10
4.3.8 Documentation Supplied to Personnel 10
4.4 Audit Logging Procedures 11
4.4.1 Types of Events Recorded 11
4.4.2 Frequency of Processing Log 11
4.4.3 Retention Period for Audit Log 11
4.4.4 Protection of Audit Log 12
4.4.5 Audit Log Backup Procedures 12
4.4.6 Audit Collection System 12
4.4.7 Notification to Event-causing Subject 12
4.4.8 Vulnerability Assessments 12
4.5 Compromise and Disaster Recovery 12
4.5.1 Incident and Compromise Handling Procedures 12
4.5.2 Corrupted Computing Resources, Software, and/or Data 13
4.5.3 Entity Private Key Compromise Procedures 13
4.5.4 Business Continuity and IT Disaster Recovery Capabilities 13
4.6 Entity Termination 14
5 Technical Security Controls 14
5.1 Key Pair Generation and Installation 14
5.1.1 Key Pair Generation 14
5.1.2 Public Key Delivery 15
5.1.3 Public Key Parameters Generation and Quality Checking 15
5.1.4 Key Usage Purposes 15
5.2 Private Key Protection and Cryptographic Module Engineering Controls 15
5.2.1 Cryptographic Module Standards and Controls 15
5.2.2 Private Key (m-of-n) Multi-person Control 16
5.2.3 Private Key Escrow 16
5.2.4 Private Key Backup 16
5.2.5 Private Key Storage on Cryptographic Module 16
5.2.6 Private Key Archival 16
5.2.7 Private Key Transfer into or from a Cryptographic Module 16
5.2.8 Method of Activating Private Key 17
5.2.9 Method of Deactivating Private Key 17
5.2.10 Method of Destroying Private Key 17
5.3 Other Aspects of Key Pair Management 17

5.3.1 Public Key Archival 17
5.3.2 Key Usage Periods 17
5.4 Activation Data 17
5.4.1 Activation Data Generation and Installation 18
5.4.2 Activation Data Protection 18
5.5 Computer Security Controls 18
5.6 Network Security Controls 18
5.7 Timestamping 18
5.8 Life Cycle Technical Controls 19
5.8.1 System Development Controls 19
5.8.2 Security Management Controls 19
5.8.3 Life Cycle Security Controls 19
6 Zone Signing 19
6.1 Key Lengths, Key Types and Algorithms 19
6.2 Authenticated Denial of Existence 20
6.3 Signature Format 20
6.4 Zone Signing Key Roll-over 20
6.5 Key Signing Key Roll-over 20
6.6 Signature Life-time and Re-signing Frequency 21
6.7 Verification of Zone Signing Key Set 22
6.8 Verification of Resource Records 22
6.9 Resource Records Time-to-Live 22
7 Compliance Audit 22
7.1 Frequency of Entity Compliance Audit 22
7.2 Identity/Qualifications of Auditor 23
7.3 Auditor's Relationship to Audited Party 23
7.4 Topics Covered by Audit 23
7.5 Actions Taken as a result of Deficiency 23
7.6 Communication of Results 24
8 Legal Matters 24
8.1 Fees 24
8.2 Financial Responsibility 24
8.3 Confidentiality of Business Information 24
8.3.1 Scope of Confidential Information 24
8.3.2 Types of Information not Considered Confidential 24
8.3.3 Responsibility to Protect Confidential Information 25
8.4 Privacy of Personal Information 25
8.4.1 Information Treated as Private 25
8.4.2 Information not Deemed Private 25
8.4.3 Responsibility to Protect Private Information 25
8.4.4 Disclosure Pursuant to Judicial or Administrative Process 25
8.5 Limitations of Liability 25
8.6 Term and Termination 26
8.6.1 Term 26

8.6.2 Termination..... 26
8.6.3 Dispute Resolution Provisions..... 26
8.6.4 Governing Law..... 26

1 Introduction

This document is the DNSSEC Policy and Practice Statement (DPS) for ".CN" top-level domain Registry Services. It states the practices and provisions that CNNIC employs in providing ".CN" zone signing and distribution services.

This document conforms to the RFC-draft DNSSEC Policy & Practice Statement Framework. The DPS is one of several documents relevant to the operation of the ".CN" TLD.

1.1 Overview

Domain Name System Security Extensions (DNSSEC) are a set of specifications from IETF to add security to the DNS. DNSSEC provides a mechanism to validate DNS data to prove that it has not been modified during transit over the Internet. This is achieved by incorporating public key cryptography into the DNS hierarchy, forming a chain of trust originating from the root zone.

DNS was not originally designed with strong security mechanisms to provide integrity and authenticity of DNS data. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system. DNSSEC addresses these vulnerabilities by adding data origin authentication, data integrity verification and authenticated denial of existence capabilities to the DNS.

This DPS is specifically applicable to all DNSSEC related operations performed by CNNIC for the ".CN" TLD. More generally, this document will provide the governing policies and provisions related to the management, security and technical specifications of the ".CN" Key Signing Key (KSK) and Zone Signing Key (ZSK). This document will be under the control and management of CNNIC. Information in this document and subsequent documents will be made public as required.

1.2 Document Name and Identification

DNSSEC Policy and Practice Statement for ".CN" Zone (".CN" DPS)

Version: 1.0

1.3 Community and Applicability

In this section, associated entities and their roles are described.

1.3.1 Registry

CNNIC is the Registry for the ".CN" top-level domain. The Registry administrates registrations of ".CN" domain names and operates DNS servers for the ".CN" zone, etc. As for ".CN" DNSSEC Service, the Registry generates signing keys (KSK and ZSK) of the ".CN" zone and completes zone signing for the ".CN" zone. Further, through registering delegation signer (DS) records of the Registry into the root zone, the Registry enables origin authentication and data integrity verification of records in the ".CN" zone by using KSK of the root zone as a trust anchor.

1.3.2 Registrar

The Registrar of the ".CN" top-level domain is an entity who has concluded an agreement with the Registry for agency operations on ".CN" top-level domain name registrations. The Registrar is responsible for the administration and management of domain names on behalf of the Registrant.

The Registrar handles the registration, maintenance and management of a Registrant's domain name and is an accredited ".CN" partner. The Registrar is responsible for securely authentication of the Registrant of a domain. The Registrar is responsible for adding, removing or updating specified DS records for each domain at the request of the Registrant.

1.3.3 Registrant

A Registrant is an entity that controls a domain name. Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the Registrar. The Registrant is responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

The Registrant may do all the above things itself. But in some cases, Registrant requests "DNS Provider" (maybe Registrar or other entity), who provides operation services for authoritative DNS servers, to generate signing keys, compose digital signatures on Registrant Zone and generate DS record(s).

1.3.4 Relying Party

Relying party is all the entity related to ".CN" DNSSEC Service, including DNS Providers, caching DNS server operators and users who utilize their services. Here we refer to the DNS Provider who manages Registrant Zone as "Registrant Zone Manager". In some cases, Registrant

him/her-self may be Registrant Zone Manager.

1.3.5 Applicability

The DPS is applied to ".CN" zone. DNS users are able to conduct origin authentication and verify data integrity of DNS responses from the ".CN" zone. Registrant Zones are under Registrant's policy and outside the scope of ".CN" DPS.

1.4 Specification Administration

This DPS will be periodically reviewed and updated, as appropriate by the CNNIC Policy Management Authority (PMA). The PMA is responsible for managing the DPS and should be considered the point of contact for all matters related to the DPS.

1.4.1 Specification Administration Organization

China Internet Network Information Center (CNNIC)
4 South 4th street, zhonguancun
Haidianqu, Beijing
P.R. China

1.4.2 Contact Information

DNSSEC PMA (Policy Management Authority):
China Internet Network Information Center. (CNNIC)
4 South 4th street,zhonguancun
Haidianqu,Beijing
P.R.China
Telephone: +86-10-58813200
Fax: + 86-10-58812666-123
http://www.cnnic.cn
dnssec-pma@cnnic.cn

1.4.3 Specification Change Procedures

Amendments to this DPS are made by the CNNIC DNSSEC Policy Management Authority (PMA). Amendments will be in the form of either a document containing an amended form of the DPS or

an update. Amended versions and updates will be linked to the DNSSEC Practices Updates and Notices section of the CNNIC website located at: http://www.cnnic.cn/dnssec/docs/.CN.dnssec-dps.pdf.

Only the most recent version of this DPS is applicable.

CNNIC reserves the right to amend the DPS without notification for amendments that are not designated as significant. It is at the sole discretion of the PMA to designate changes as significant, and in such cases CNNIC will give a notice. Any changes will be approved by the PMA and may be effective immediately upon publication.

2 Publication and Repositories

2.1 Publication site

CNNIC publishes the DPS in the docs section of CNNIC's website, at: http://www.cnnic.cn/dnssec/docs/.CN.dnssec-dps.pdf.

2.2 Publication of Key Signing Keys (KSK)

The public key of the ".CN" KSK (DS record) will be published in the root zone, and will be published at: http://www.cnnic.cn/dnssec/.

2.3 Access Controls on Repositories

Information published in the docs portion of the CNNIC website is publicly accessible information. Read-only access to such information is unrestricted. CNNIC has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Operational Requirements

3.1 Meaning of Domain Names

The DNSSEC deployment policy of ".CN" TLD provides DNSSEC support for domain names of and below the second level that are ended with ".CN". But this requires that all applicants and registrars for domain names ended with ".CN" should submit to CNNIC both legal domain

names which conform to the rules for domain name nomenclature and legally authoritative resource records.

3.2 Activation of DNSSEC for Child Zone

Based on the fact that a child zone has been duly delegated by CNNIC, ".CN" TLD can provide DNSSEC support for the child zone after receiving its delegation singer (DS). CNNIC will write the DS submitted by the child zone into the zone file of ".CN" TLD. Users can query the record via the recursive server.

3.3 Identification and Authentication of Child Zone Manager

It is the responsibility of the Registrar to securely identify and authenticate the Registrant through a suitable mechanism, and in compliance with the stipulations in the contract between CNNIC and the Registrar.

3.4 Registration of Delegation Signer (DS) Resource Records

The ".CN" TLD registry does not require secondary or lower domain names of ".CN" to support DNSEEC. Whether it should be supported by these domain names totally depends on the registrant. To facilitate the submission of DS of ".CN" child zones and realize the binding of DS records with domain name information, CNNIC needs to open DS registration channels to domain name registrars.

CNNIC provides the following two methods for domain name registrars:

1) Registrars can submit DS records via a special Web system;
2) They can submit DS records via EPP (RFC5910).

3.5 Method to Prove Possession of Private Key

The Registry does not conduct any controls with the aim of validating the Registrant as the manager of a private key. The Registrar is responsible for conducting the controls that are required and those deemed necessary.

3.6 Removal of DS Resource Records

To keep zone files clean, prevent useless DS storage from causing expansion of zone files and prevent zone file signing from taking too much time, the administrator of ".CN" TLD zone files may remove a DS resource record in the following two cases:

1) When a ".CN" child zone asks for DS updating , the old DS record is removed;
2) When a ".CN" child zone cancels its DNSSEC deployment and goes into the non-DNSSEC-service state.

The old DS record is removed 10 days later instead of being removed immediately.

4 Management, Operational and Physical Control

4.1 Physical Controls

4.1.1 Site Location and Construction

To avoid unauthorized operations and leakage of sensitive information, DNSSEC operation and maintenance of the ".CN" TLD is carried out in a strictly protected physical environment. CNNIC has established a sound backup system for all DNSSEC-related services in the IDC of each secondary operation center, where the level of physical protection is the same as that of the primary operation center.

4.1.2 Physical Access

Important equipment such as servers and hardware security modules (HSM) used for ".CN" TLD DNSSEC deployment must be placed in a IDC with strict access control and only authorized persons may go into the machine room.

To prevent outside electromagnetic signals from interfering with the generation of keys, the HSM is kept in a locked electro-magnetic shielding cabinet. Both the HSM and the cabinet are placed in a separate room with access control measures and only authorized persons may get access to the cabinet.

4.1.3 Power and Air Conditioning

CNNIC facilities are equipped with two separate power supply systems (one working and the other standby) and heating/ventilation/air conditioning system to control temperature and

relative humidity so that uninterrupted operation can be ensured.

4.1.4 Water Exposures

CNNIC has taken reasonable measures to prevent the ".CN" service system from being exposed to water.

4.1.5 Fire Prevention and Protection

CNNIC has taken reasonable fire prevention and protection measures. In case of fire, smoke and flames can soon be brought under control. All these measures meet the requirements of local laws and regulations for fire control and prevention.

4.1.6 Media Storage

All software, data-containing media, auditing information, archives and the corresponding backup information are stored in a secure local or remote device for appropriate physical and logical access to prevent them from accidental damage (water, fire, electromagnetic fields, etc.) or from being exposed to unauthorized personnel.

4.1.7 Waste Disposal

Before being discarded or dumped, sensitive paper documents and materials shall be shredded in a paper shredder; CD-ROMs, magnetic disks, etc., shall be demagnetized in a demagnetizer; HSMs and other equipment shall be physically destroyed or zeroed as per the manufacturer's instruction. Other useless articles or goods shall be disposed of in accordance with the general procedures of CNNIC.

4.1.8 Off-site Backup

Key system data, auditing log data and other important information related to ".CN" TLD DNSSEC service will be stored in the off-site backup media of the primary operation center and the secondary operation centers in a physically isolated manner.

4.2 Procedural Controls

CNNIC will formulate strict procedures to control the construction and deployment of hardware

facilities. CNNIC will also work out relevant specifications and procedures to control the deployment of software and to standardize all operations.

4.2.1 Trusted Roles

Trusted roles refer to the persons who, during ".CN" TLD DNSSEC operation, are permitted to operate HSMs, generate keys and participate in generating and signing zone files. To be specific, these roles include the following two types:

1) System administrators;
2) System operators.

Each type of the above roles is not authorized to do the job of the other.

CNNIC will select and train the trusted roles in basic DNSSEC skills so that they will be competent for their later work. Excellent personnel from these trusted roles will be selected to be the key administrators (defined in 5.1.1).

4.2.2 Number of Persons Required Per Task

In actual operation, the number of persons to play each of the trusted roles described in Section 4.2.1 is as follows:

1) During construction of DNSSEC hardware equipment and environment, at least one person per role shall be present at the site, and one of them shall be involved in the entire process of construction and deployment.
2) During DNSSEC software service and deployment, at least one person per role shall be present at the site, and one system administrator shall be involved in the entire process of software deployment. The System operator(s) shall check the correctness of software deployment.
3) Each time keys are generated or backed up, at least three persons shall be present at the site (they are all the current key administrators, please see 5.1.1). At least, two of them shall be system administrators and one shall be System operator.

4.2.3 Identification and Authentication for Each Role

CNNIC will select trusted persons for the implementation of ".CN" TLD DNSSEC deployment according to their work experience, qualifications and job duties.

The selected persons shall sign a confidentiality agreement with CNNIC to undertake all the management duties authorized by the agreement. They shall promise to keep confidential the

information related to ".CN" TLD DNSSEC deployment strategies. They shall undertake not to disclose the information to any third party, or else they shall assume corresponding legal liabilities.

4.2.4 Tasks Requiring Separation of Duties

1) Construction of DNSSEC hardware equipment and environment
2) Deployment of DNSSEC software service
3) operation of keys

4.3 Personnel Controls

4.3.1 Qualifications, Experience, and Clearance Requirements

CNNIC will select a number of trusted roles for the implementation of ".CN" TLD DNSSEC deployment according to their work experience, qualifications and job duties. These persons shall promise to keep confidential the details related to ".CN" TLD DNSSEC deployment and not to disclose the information to any third party.

4.3.2 Background Check Procedures

All candidates for ".CN" trusted roles shall be subject to an investigation into and assessment of their backgrounds of at least the most recent three years.
Before being appointed as a trusted role, a candidate shall be subject to an assessment of the following:

1) Certification of prior work experience
2) Certification of highest educational level
3) Investigation of any criminal record
4) Investigation of personal credit

4.3.3 Training Requirements

To improve employees' competence for and satisfaction with their work, CNNIC will provide basic technical training for them and adjust or update the training courses when necessary.
Customized to meet the real needs of CNNIC employees, the training courses cover the following contents:

1) Basic concepts of DNS/DNSSEC;
2) An introduction of job duties;
3) Use and maintenance of software and hardware that have been deployed;
4) Procedures for disaster recovery and business continuity management.

4.3.4 Retraining Frequency and Requirements

Every two years or when major adjustments are made to the system framework CNNIC will provide additional training or testing for its employees to improve their competence for and satisfaction with the work.

4.3.5 Job Rotation Frequency and Sequence

CNNIC employees will mutually exchange their functional roles on a rotating basis when necessary.

4.3.6 Sanctions for Unauthorized Actions

Sanctions will be meted out for unauthorized actions in accordance with the employment agreement. Serious negligence may lead to termination of the employment.

4.3.7 Contracting Personnel Requirements

In some cases temporary employees are needed for the DNSSEC operation and maintenance of ".CN" TLD. To be selected as trusted roles, these employees must be subject to background investigation and then sign a confidentiality agreement which is the same as permanent employees sign. Their work must be under the guidance and supervision of other trusted roles.

4.3.8 Documentation Supplied to Personnel

CNNIC provides necessary training and documents for its employees to enhance their competence for and satisfaction with the work.

4.4 Audit Logging Procedures

4.4.1 Types of Events Recorded

Auditing is performed manually or automatically. CNNIC will record the following major events:

1) Events related to ".CN" KSK&ZSK lifecycle management, including:
   - Generation, backup, storage, archived and deletion of keys;
   - Exporting of the public keys;
   - Events related to HSM lifecycle management;
2) Events related to management of KSK&ZSK signing, including:
   - Activation of keys;
   - Acceptance and confirmation of public key signing information;
   - Success or failure of the signing process;
   - Events of key rotation;
3) Security-related events, including:
   - Successful or unsuccessful system access attempts;
   - All operations performed by trusted roles;
   - Writing, reading and deleting security-sensitive files;
   - System breakdowns and emergent failures;
   - IDC entries;
   - System changes or updates;
   - Handling of failures.

These records should include the date and time when the record is made, the type and number of the record, etc.

CNNIC will periodically audit these records for security sake and record and solve any problem found in the auditing process.

4.4.2 Frequency of Processing Log

CNNIC analyzes some of the above records in a real-time manner through a log analysis system. Wherever there is any problem concerning DNSSEC service, CNNIC will immediately check the corresponding records.

4.4.3 Retention Period for Audit Log

Audit logs are electronically stored in the log system for at least one month. After that, the

logs will be archived and kept in the tape library for at least 10 years.

4.4.4 Protection of Audit Log

The log system and tape library will reject unauthorized access, modification and deletion.

4.4.5 Audit Log Backup Procedures

Logs kept in the tape library will be sent to the secondary operation centers on a monthly basis for backup.

4.4.6 Audit Collection System

Audit information will be automatically generated and recorded at the application, network and operation system levels. Audit data will be manually generated and recorded by CNNIC employees.

Electronic information will be incrementally backed up in the operation center; paper records will be archived by type and entry and properly kept.

4.4.7 Notification to Event-causing Subject

When the audit collection system records a certain event, it is unnecessary to notify the individual, organization, equipment or application program that causes the event.

4.4.8 Vulnerability Assessments

Records of the above event may serve as the necessary material and basis for assessing the vulnerability of ".CN" TLD DNSSEC service operation.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and Compromise Handling Procedures

Database data is backed up in the secondary operation centers so that original zone files can be directly generated in case of any compromise or disaster.

Keys are also backed up in the HSM of the secondary operation centers so that they are available when a disaster occurs to the primary operation center. See Section 5.2.4 for more

detail.

4.5.2 Corrupted Computing Resources, Software, and/or Data

In case of corrupted computing resources, software and/or data, CNNIC will handle the problem in accordance with the procedures specified in the ".CN" Registry Emergency Response Program. If service cannot be resumed or failure cannot be removed in a short time, CNNIC will consider switching services to the secondary operation center by adopting the disaster recovery mechanism.

4.5.3 Entity Private Key Compromise Procedures

1) ZSK Compromise

In case the ZSK is cracked or leaked out a new ZSK shall be generated and signing shall be performed using the new key. The old ZSK will be kept for 10 days and then deleted.

2) KSK Compromise

In case the KSK is cracked or leaked out, it must be updated immediately. In such a case, CNNIC will generate and announce a new KSK as quickly as possible and submit to the root zone for a DS record corresponding to the newly-generated KSK. The root zone will send the new DS record to all authoritative servers and delete the old DS record. Finally, CNNIC will delete the old KSK and use the new one for ZSK re-signing. The information of emergent KSK update will be announced through CNNIC official website http://www.cnnic.cn and the CNNIC DNSSEC mail list dnssec-pma@cnnic.cn. Information of the leaked KSK and its signature will be kept by CNNIC for 30 days and then deleted.

4.5.4 Business Continuity and IT Disaster Recovery Capabilities

CNNIC has formulated a ".CN" registry business continuity plan in accordance with the Continuity Management Procedures, a second-level document of CNNIC information security management system (ISMS). Formulated with reference to the requirements of ISO27001 on continuity, the Continuity Management Procedures clarifies that the aim of continuity management is to combine prevention with resumption of control; proactively guard against and deal with IT-related emergent events; avoid interruption of operational activities; confine the impact of IT-related emergent events on CNNIC to within a bearable limit; and ensure the continuity of core services, by establishing a continuity management system featured by "sound mechanism, centralized leadership, clear accountability, proactive prevention, quick response and efficient

disposal". The Operation Continuity Management Procedures also clarifies the methods for and contents of the implementation of the registry continuity plan.

The ".CN" Registry Emergency Response Program has designed specific procedures for various pre-set scenarios and clarified the operations of personnel on different work posts in handling emergent events. The pre-set scenarios are designed based on the threats identified through risk analyses and CNNIC's experience in operating the ".CN" domain name system. These scenarios mainly include those where security events are very likely to occur or where events that once occurred may lead to "significant" or more serious security events. They also include the scenarios where security events are not likely to occur but once they occur, they will constitute an extremely great security threat. Meanwhile, pre-set emergent scenarios will be enriched according to real situations so that the Emergency Response Program can be continuously improved.

4.6 Entity Termination

If CNNIC decides to terminate ".CN"TLD registry service, it shall notify ICANN of its decision in advance and the transition process can be started after ICANN has selected a new Registry. To ensure the availability and continuity of registry service during the transition process, CNNIC shall have consultations with the new Registry about key rotation.

5 Technical Security Controls

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

All pairs of keys (ZSK and KSK) in use are generated in the HSM in a secure way. The cryptographic module meets the standard of Chinese authorities and relevant international standards. Five key administrators account are generated during the HSM initialization process, and only more than half of them have passed identity authentication can the HSM be accessed.

Generation of keys is performed by well-trained key administrators. At least three key administrators (Appointing at least two system administrators and at least one System operator is allowed in an emergency situation) will be involved in the entire process of key generation and designated auditing personnel will be present to supervise and record the process.

5.1.2 Public Key Delivery

Each public key of KSK generated will be exported from the HSM and its validity will be verified by System operators. Then it will be sent to ICANN and at the same time the information will be published on the official website of CNNIC.

5.1.3 Public Key Parameters Generation and Quality Checking

Basic parameters for generation of keys used for the DNSSEC deployment of ".CN" TLD are as follows:

1) KSK generation algorithm and key length: RSA-SHA256 2048bits
2) ZSK generation algorithm and key length: RSA-SHA256 1024bits

In addition CNNIC will adjust the above parameters when necessary according to real situations to ensure that the keys are sufficiently safe and protect them from being cracked.

5.1.4 Key Usage Purposes

All keys generated will be used only for the purpose of ".CN" TLD deployment rather than any other purposes.

ZSK is used for signing each DNS resource records set (RRset) of ".CN" TLD zone files.

KSK is used for signing DNSKEY RRset of ".CN" TLD zone files.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

After being generated, keys (ZSK and KSK) are directly stored in the HSM.

5.2.1 Cryptographic Module Standards and Controls

The cryptographic module meets the standard of Chinese authorities and relevant international standards. Five key administrators account are generated during the HSM initialization process, and only more than half of them have passed identity authentication can the HSM be accessed.

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

The HSM provides key backup functions. It divides an encrypted key into 5 segments and stores

them in five different smart cards, each kept by an key administrator. In emergent cases, the key in the HSM can be restored using any 3 of the segments.

5.2.3 Private Key Escrow

CNNIC (the Registry) does not escrow private keys.

5.2.4 Private Key Backup

After being generated, private keys are backed up in another HSM with identical configuration using a special key-backup card.

In addition CNNIC will send at least three key administrator (Appointing at least one system administrators is allowed in an emergency situation) carrying special key-backup card to the secondary operation centers on a regular basis to back them up in the HSM of the secondary operation center.

5.2.5 Private Key Storage on Cryptographic Module

It is forbidden to access or read private keys in any plaintext form but it is permitted to back up their information in special key-backup card in an cryptographic manner.

5.2.6 Private Key Archival

Private keys are used for backup only and shall not be used in any other form. Meanwhile, information of private key backup will be recorded and a corresponding archive will be created for this purpose.

5.2.7 Private Key Transfer into or from a Cryptographic Module

The HSM that generates private keys supports zone signing (encryption) functions. After a private key is generated, the HSM will directly export it to the cryptographic module for use via an internal physical process unit.

5.2.8 Method of Activating Private Key

Private keys are automatically activated by the HSM based on pre-set timing parameters without any need for human intervention.

5.2.9 Method of Deactivating Private Key

Private keys are automatically deactivated by the HSM based on pre-set timing parameters when they expire, without any need for artificial intervention.

5.2.10 Method of Destroying Private Key

Private keys stored in the HSM are automatically destroyed when they expire, without any need for human intervention. Private keys stored in the key-backup card and backup HSM are deleted in a standard manner as specified, and such a process is supervised and recorded by designated personnel.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

Public keys will be archived together with other types of traceable information such as log data.

5.3.2 Key Usage Periods

When keys expire they will be deleted from the signing system and will not be used any more. The usage period of ZSK is 3 months and that of KSK is 12 months. The record of signing is valid for 30 days.

5.4 Activation Data

The activation data is the personal passphrase for the card of each key administrator that is used to activate the HSM.

5.4.1 Activation Data Generation and Installation

Each key is responsible for creating their own activation data pursuant to the applicable requirements of at least nine characters of varying nature.

5.4.2 Activation Data Protection

Key administrators are required to safeguard their card and sign an agreement acknowledging their responsibilities.

Each Key administrator is responsible for protecting their activation data in the best possible way. On the suspicion of compromised activation data, the Key administrator must immediately change it.

5.5 Computer Security Controls

In DNSSEC deploying ".CN", specific servers (for zone file generation) are allowed to access HSM. The authority of access to such servers should be restricted and controlled so that only trusted roles can get access to them. Access control policies should also be made for other servers that communicate with the above servers to ensure their security.

5.6 Network Security Controls

All pairs of keys are generated in HSM. To ensure its security and prevent other servers or equipment in the network from accessing it, a separate subnet will be built for deploying the key generation system. The security of the subnet will be ensured by a firewall and other security means.

5.7 Timestamping

UTC is adopted for timing the validity of all logs, signing records, etc., related to the signing system.

5.8 Life Cycle Technical Controls

5.8.1 System Development Controls

All source codes are stored in control systems of the same version and these codes are backed up and archived periodically.

5.8.2 Security Management Controls

CNNIC creates a hash of all software packages installed on production systems. This hash may be used to verify the integrity of such software. The monitoring system will alert when critical software packages are modified.

5.8.3 Life Cycle Security Controls

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system will be applied after formal testing and approval. The origin of all software and firmware will be securely authenticated by available means.
Critical hardware components of the HSM will be procured directly from the manufacturer and transported in tamper-evident bags to their destination in the secure facility. Any hardware will be decommissioned well before the specified life time expectancy.

6 Zone Signing

This part deals with technical parameters of keys, authenticated denial of existence, the lifecycle of keys and rotation policies for DNSSEC deployment.

6.1 Key Lengths, Key Types and Algorithms

For ".CN" TLD DNSSEC deployment, the algorithms for key generation and the corresponding key lengths are as follows:

1) KSK generation algorithm and key length: RSA-SHA256 2048bits
2) ZSK generation algorithm and key length: RSA-SHA256 1024bits

6.2 Authenticated Denial of Existence

To prevent unauthorized people from viciously scanning ".CN" TLD zone files and protect ".CN" TLD zone data, NSEC3 (RFC 5155) is adopted for DNSSEC deployment.

6.3 Signature Format

The signature format in ".CN" TLD zone files conforms to the standard format defined in RFC4034.

6.4 Zone Signing Key Roll-over

To prevent the keys from being cracked or leaked out, ZSK should be replaced and rotated on a regular basis. The ZSK roll-over policy is to adopt a pre-publish mechanism (RFC4641). The validity period of each ZSK generated is 100 days and the roll-over cycle is 90 days.

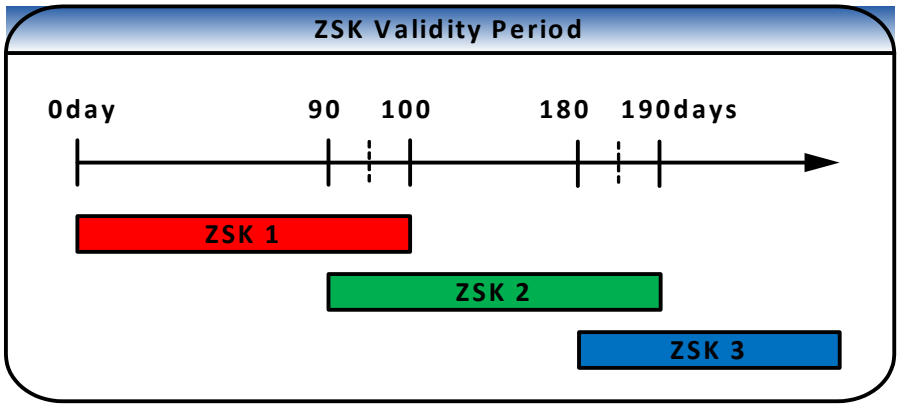

Figure 1 ZSK Roll-over Cycle

6.5 Key Signing Key Roll-over

As the foundation of the chain of trust of DNSSEC, the KSK should also be rotated on a regular basis to prevent it from being cracked or leaked out. The KSK roll-over policy is to adopt a double-signature mechanism (RFC4641). The validity period of each KSK generated is 13 months and the roll-over cycle is 12 months. During the KSK roll-over period, the ".CN" zone administrator shall submit the DS record related to the new KSK to the root zone administrator so as to maintain the integrity of the chain of trust.

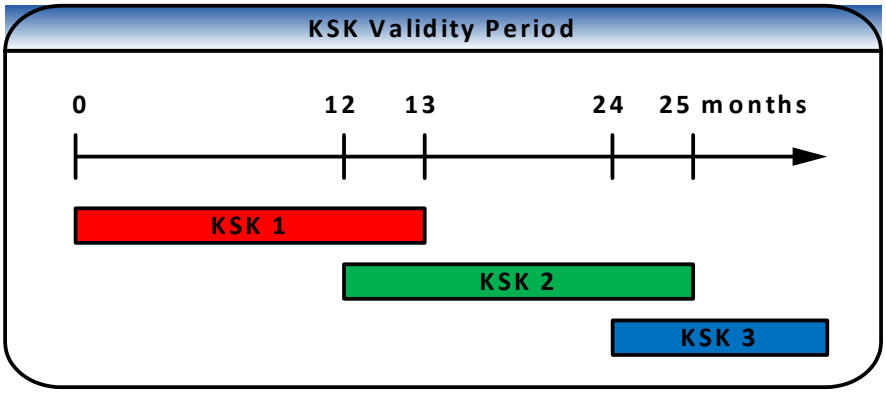

Figure 2 KSK Roll-over Cycle

6.6 Signature Life-time and Re-signing Frequency

The signature validity period, without exception, is 30 days for all resource records (RRSIG, RFC4034) of ".CN" TLD zone signatures, all of which shall be re-signed when they expire. So the re-signing frequency is once every 30 days.

In addition, re-signing is also necessary each time ZSK or KSK is rotated.

Zone signing will be executed in the HSM, for which the basic procedures are as follows:

1) The hidden primary master obtains resource records from the ".CN" registration database and generates the original zone file;
2) The hidden primary master securely sends the original zone file to HSM;
3) HSM reads the configuration files for zone signing and generates the keys needed, including KSK and ZSK;
4) HSM executes zone signing using ZSK and KSK;
5) When zone signing is completed, HSM sends the files that have been signed back to the hidden primary master;
6) The zone files that have been signed are loaded onto the hidden primary master, which will then update data to the secondary master servers.

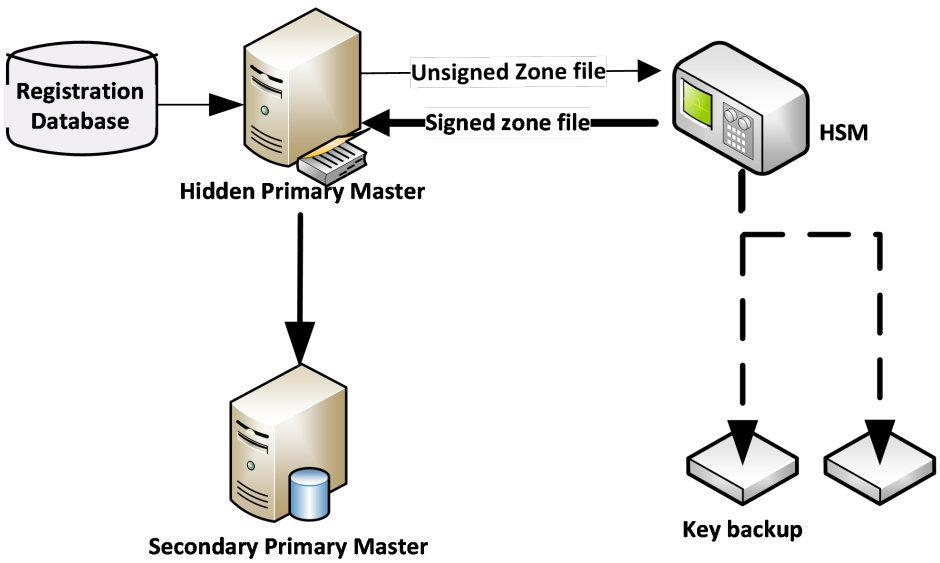

Figure 3 ".CN" TLD Zone File Signing

6.7 Verification of Zone Signing Key Set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. This is done by verifying the

chain from DS in the root zone to KSK, ZSK and the signature over the ".CN" SOA.

6.8 Verification of Resource Records

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

6.9 Resource Records Time-to-Live

The TTL of DNSSEC-related resource records in ".CN" TLD zone files is set to be 6 hours, which is consistent with the TTL of other DNS resource records in the zone files.

7 Compliance Audit

7.1 Frequency of Entity Compliance Audit

Compliance audits are conducted at least annually at the sole expense of the audited entity.

7.2 Identity/Qualifications of Auditor

CNNIC's compliance audits are performed by a public accounting firm that demonstrates proficiency in DNSSEC public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

7.3 Auditor's Relationship to Audited Party

Compliance audits of CNNIC's operations are performed by a public accounting firm that is independent of CNNIC. Third party auditors do not participate in the multi-person control for the ".CN" ZSK and KSK.

7.4 Topics Covered by Audit

The scope of CNNIC's annual compliance audit includes all DNSSEC operations such as key environmental controls, key management operations, infrastructure/administrative controls, KSK and ZSK and signature life cycle management and practices disclosure.

7.5 Actions Taken as a result of Deficiency

With respect to compliance audits of CNNIC's operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by CNNIC management with input from the auditor. CNNIC management is responsible for developing and implementing a corrective action plan. If CNNIC determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the ".CN" KSK and/or ZSK, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, CNNIC management will evaluate the significance of such issues and determine the appropriate course of action.

7.6 Communication of Results

The auditing manager shall submit a written report of the audit results to CNNIC not later than 30 calendar days after the audit.

8 Legal Matters

8.1 Fees

".CN" Regsitry does not charge Registrars any fees for DNSSEC.

8.2 Financial Responsibility

Not applicable.

8.3 Confidentiality of Business Information

8.3.1 Scope of Confidential Information

The following records shall be kept confidential and private (Confidential/Private Information):

1) Private keys and information needed to recover such Private Keys
2) Transactional records (both full records and the audit trail of transactions)
3) Audit trail records created or retained by CNNIC
4) Audit reports created by CNNIC (to the extent such reports are maintained), and their respective auditors (whether internal or public)
5) Contingency planning and disaster recovery plans
6) Security measures controlling the operations of CNNIC hardware and software and the administration of DNS Keys

8.3.2 Types of Information not Considered Confidential

All information pertaining to the database of top level domains is public information. Public Keys, Key Revocation, and other status information, as well as CNNIC publication and information contained within them are not considered Confidential/Private Information.

8.3.3 Responsibility to Protect Confidential Information

CNNIC secures confidential information against compromise and disclosure to third parties.

8.4 Privacy of Personal Information

8.4.1 Information Treated as Private

To the extent CNNIC receives or processes, on behalf of a customer, personally identifiable information (PII) in the course of providing ".CN" Zone services, such PII is treated as private in accordance with the terms of CNNIC's agreements with Registrars and CNNIC's Privacy Policy.

8.4.2 Information not Deemed Private

Subject to applicable laws, all information required to be published as part of a whois database is not deemed private.

8.4.3 Responsibility to Protect Private Information

In providing ".CN" Zone services, CNNIC acts as a data controller, and any obligations that CNNIC may have with respect to any personally identifiable information is governed, subject to applicable law, by the terms of CNNIC's agreements with registrars and to the extent not governed by any applicable Registry Registrar agreement.

8.4.4 Disclosure Pursuant to Judicial or Administrative Process

CNNIC shall be entitled to disclose Confidential/Private Information if, in good faith, CNNIC believes that such 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

CNNIC shall not be liable for any financial loss or losses arising from incidental damage or impairment resulting from its performance of its obligations hereunder or the ".CN" Zone Manager's or the ".CN" Zone KSK and ZSK Operator's performance of their respective obligations under DNSSEC Practice Statement for the ".CN" Zone KSK and ZSK Operator. No other liability, implicit or explicit, is accepted.

8.6 Term and Termination

8.6.1 Term

The DPS becomes effective upon publication on the CNNIC website. Amendments to this DPS become effective upon publicationon the CNNIC website.

8.6.2 Termination

This DPS is 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. Disputes involving CNNIC require an initial negotiation period of sixty (60) days followed by litigation in the Beijing Haidian District intermediate people's court, PRC.

8.6.4 Governing Law

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