DNSSEC Practice Statement for 政府 zone

1. INTRODUCTION

This document is the TWNIC DNSSEC Practice Statement (DPS) for 政府 TLD, it states the practices and provisions that TWNIC employ in providing 政府 TLD Key Signing and Key Distribution services.

1.1. Overview

DNSSEC is a set of extensions to the DNS protocol. The foundation of DNSSEC is defined in RFCs 4033, 4034, and 4035 and notably extended by RFC 5155.

There is one DNSSEC resource record which will appear in registration activity, the DS resource record. TWNIC completely supports DS field in database and EPP. Registrars can upload DS RR to registry via EPP. Once TWNIC's zone file is established, all the related zone files will be produced and DS will be automatically put in the zone file through BIND signing tools.

1.2. Document Name and Identification

DNSSEC Practice Statement for 政府 zone
Version: 1.0.1
Date: 2014/10/17

1.3. Community and Applicability

1.3.1. 政府 zone Administrator

Net-Chinese is the Registry for the 政府 TLD. The Registry administrates registrations of 政府.

1.3.2 政府 zone Maintainer

TWNIC is the 政府 zone maintainer to operate DNS servers for 政府 zone.

1.3.3. 政府 server Operators

TWNIC is the only operator for 政府 DNS servers.

1.3.4. 政府 Zone Key Signing Key Operator

The 政府 Zone Key Signing Key Operator is TWNIC performing the function of generating the 政府 Zone's Key Signing Key (KSK) and signing the 政府 keyset using the KSK. The 政府 Zone Key Signing Key Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the Key Signing Key to the parent zone.

The 政府 Zone KSK (政府 KSK) operator is responsible for:

(1) Generating and protecting the private component of the 政府 KSK.

(2) Securely importing public key components from the 政府 Zone Signing Key (ZSK) operator.

(3) Authenticating and validating the public 政府 ZSK keyset.

(4) Securely signing the 政府 ZSK and KSK keyset (i.e., all DNSKEY records).

(5) Securely transmitting the signed 政府 DNSKEY Resource-Record Set to the 政府 ZSK operator.

(6) Securely exporting the 政府 KSK public key components.

(7) Creating a DS record from the KSK public key and submitting it to IANA for insertion into the root zone.

(8) Issuing an emergency key roll-over within reasonable time if any KSK associated with the zone is lost or suspected to be compromised.

1.3.5. 政府 Zone Signing Key Operator

The 政府 Zone Signing Key Operator is TWNIC performing the function of generating the 政府 Zone's Zone Signing Key (ZSK) and signing the 政府 Zone File using the ZSK.

The 政府 Zone Signing Key Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the Zone Signing Key to the 政府 Zone Key Signing Key Operator for signing.

The 政府 Zone ZSK (政府 ZSK) operator is responsible for:

(1) Generating and protecting the private component of the 政府 ZSK.

(2) Securely exporting and transmitting the public 政府 ZSK component to the 政府 KSK Operator.

(3) Securely importing the signed 政府 DNSKEY Resource Record Set from the 政府 KSK operator.

(4) Signing the 政府 Zone's authoritative resource records omitting the DNSKEY resource record.

(5) Issuing an emergency key roll-over within a reasonable amount of time if any ZSK

associated with the zone is lost or suspected to be compromised.

1.3.6. Child zone manager

The child zone (政府 Domain Name) managers are trustees for the delegated domain, and as such are responsible for providing their own DNS services and operating subordinate DNS servers. In regard to DNSSEC, the child zone manager is also responsible for:
(1) Generating the keys associated with the zone using a trustworthy method.
(2) Registering and maintaining the shorthand representations of its Key Signing Key (in the form of a Delegation Signer Resource Record) in the parent zone to establish the chain of trust.
(3) Taking reasonable precautions to prevent any loss, disclosure or unauthorized use of the keys associated with the zone.
(4) Issuing an emergency key roll-over within a reasonable time if any key associated with the zone is lost or suspected to be compromised.

1.4. Specification Administration

1.4.1. Specification administration organization

Net-Chinese Co. LTD.

1.4.2. Contact information

Net-Chinese Co. LTD.
Telephone: +886 -2-2531-9696
(8:00-20:00 excluding Saturdays, Sundays, national holidays)
E-mail: service@net-chinese.com.tw

1.4.3. Specification change procedures

政府 DPS is revised annually and/or in case of arising legitimate needs. The revised 政府 DPS becomes publicly available in such a way as described in chapter 2.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

Net-Chinese and TWNIC publishes the DPS in the repository section of TWNIC's web site at http://dnssec.twnic.net.tw/政府-DPS.pdf

2.2. Publication of key signing keys

The public portion of the 政府 KSK will be published in the root zone.

2.3. Access controls on repositories

Information published in the repository portion of the TWNIC web site is publicly accessible information. Read-only access to such information is unrestricted. TWNIC 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

DNSSEC provides mechanisms for ensuring that the origin of the DNS data is consistent with the information in the registry. It does NOT provide any way of determining the legal entity behind the domain name, or the relevance of the domain name itself.

3.2. Activation of DNSSEC for child zone

DNSSEC for a child zone is activated by the publishing in the 政府 zone of a signed DS record for that child zone. The DS record is a cryptographic shorthand representation, or hash, of the child zone generated and controlled Key Signing Key. It will establish a chain of trust from the 政府 Zone to the Child Zone.

3.3. Identification and authentication of child zone manager

TWNIC does not perform any verification of the identity and authority of the child zone manager as it only applies changes received from Registrars.

3.4. Registration of delegation signer (DS) records

TWNIC applies changes to the 政府 Zone file based on requests from Registrars.

3.5. Removal of DS record

The removal of DS records (stale or active) can be requested by only the Child Zone manager.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

TWNIC installs important facilities and equipment at a place where is not easily affected by disasters including water exposures, earthquakes and fires. TWNIC also implement a physically protected environment to prevents unauthorized access to, or disclosure of sensitive information and systems.

4.1.2. Physical access

TWNIC sets up physical and environment security procedure to protect the equipment and reduce the risk of unauthorized access. The procedure includes secure areas and equipment security.

- Physical security perimeter - Physical security mechanisms include entry access control, closed circuit TV surveillance video cameras, security guards.
- Working in secure areas - guidelines for working in secure areas is documented, posted at all entry points.
- Public access delivery and loading areas - all delivery, loading, and other areas where unauthorized persons may enter the premises are controlled, and information processing facilities are isolated, to avoid unauthorized access.

4.1.3. Power and air conditioning

There are primary and backup power systems include UPS and power generator to ensure continuous, uninterrupted access to electric power and air conditioning systems to control temperature and relative humidity.

4.1.4. Water exposures and earthquakes

TWNIC takes waterproofing measures for the Important Facility Room to minimize damages due to water exposures.

4.1.5. Fire prevention and protection

TWNIC installs the Important Facilities in a fire protection zone. Further, in this zone, fire prevention measures are taken for electric power supplying facilities and air conditioning, in addition to fire alarm apparatus and fire extinguishing facilities.

4.1.6. Media storage

All media containing production software, as well as media containing data, audit, archive, and backup information is stored within TWNIC facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

4.1.7. Waste disposal

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

4.1.8. Off-site backup

TWNIC performs routine backups of critical system data, audit log data, and other sensitive information to DVDs and tapes, the two media are store in two different locations which with access control described in 4.1.2.

4.2. Procedural Controls

4.2.1. Trusted role

Trusted Persons include all employees, contractors, and consultants that have access to or control cryptographic operations that may materially affect:
- Generation and protection of the private component of the 政府 Zone Key Signing Key.
- Secure export or import of any public components.
- Zone File data.

Trusted Persons include, but are not limited to:
- Designated system administration personnel
- Crypto officers

- Cryptographic business operations personnel
- Security personnel
- System administration personnel
- Designated engineering personnel

4.2.2. Number of persons required per task

The most sensitive tasks, such as KSK-related operation including create and active key require multiple Trusted Persons. At a minimum, two trusted personnel are required to have either physical or logical access to the device.

4.2.3. Identification and authentication for each role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing TWNIC Human Resource or security functions and a check of well-recognized forms of identification. Identity is further confirmed through the background checking procedures in DPS section 4.3.

TWNIC ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:
- issued access devices and granted access to the required facilities
- issued electronic credentials to access and perform specific functions on TWNIC IT systems.

4.2.4. Tasks requiring separation of duties

Tasks requiring separation of duties include, but are not limited to, the generation, operation or destruction of 政府 Zone DNSSEC key material.

Designated audit personnel may not participate in the multi-person control for the 政府 ZSK or KSK.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

TWNIC requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof

of any government clearances or proof of any citizenship, necessary to perform operations under government contracts.

4.3.2. Background check procedures

TWNIC personnel manager performs employee background checks, which includes: personal information, previous employment, work experience, education, and criminal record.

4.3.3. Training requirements

TWNIC gives trainings to personnel in charge of 政府 DNSSEC Service as follows:
- Before having roles of operating 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. Retraining frequency and requirements

TWNIC periodically examines the necessity of re-training for personnel in charge of 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. Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions with respect to this DPS and/or other violations of TWNIC policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

4.3.7. Contracting personnel requirements

Not applicable in this document.

4.3.8. Documentation supplied to personnel

TWNIC provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

TWNIC logs the following significant events:

政府 KSK & ZSK life cycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction
- Exporting of public key components
- Cryptographic device life cycle management events

政府 KSK & ZSK signing and management events, including:

- Key activation
- Receipt and validation of signed public key material
- Successful and unsuccessful signing requests
- Key rollover events

Security-related events, including:

- Successful and unsuccessful system access attempts
- Key and security system actions performed by trusted personnel
- Security sensitive files and records read, written and deleted
- Security profile changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- Facility visitor entry/exit
- System changes and maintenance/system updates
- Incident response handling

4.4.2. Frequency of processing log

TWNIC checks the Audit Logs in a frequency sufficient to monitor promptly whether serious security incidents occur or not. If any records to be dealt with are detected, immediate notification will be made to appropriate personnel.

4.4.3. Retention period for audit log information

TWNIC keep the Audit Logs for at least 6 months in a manner of being able to

access them promptly. Archives of the Audit Logs are kept for at least 2 years.

4.4.4. Protection of audit log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

4.4.5. Audit log backup procedures

TWNIC backups the Audit Logs on DVDs and tapes periodically. The two media are store in two different locations which with access control described in 4.1.2.

4.4.6. Audit collection system

Online Audit Log are stored in Splunk database.

4.4.7. Vulnerability assessments

TWNIC implement vulnerability assessments every 6 months based on ISO27001 procedures.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

To respond to any event affecting TWNIC's DNS resolution service and domain name registration management service, TWNIC has prepared the business continuity program to establish the recovery guideline and emergency process procedure of the core businesses. Major emergency process procedures are included in the program. When the program activates, the basic services will be provided to the registrants and registrars, until the recovery is completed.

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

TWNIC will use all commercially reasonable efforts to restore critical functions. If necessary, TWNIC key compromise or disaster recovery procedures will be implemented.

4.5.3. Entity private key compromise procedures

When the KSK is compromised, TWNIC carries out the following procedures:
- Re-generation of KSK.
- Composition of signature for DNSKEY resource records by re-generated KSK.
- Replacement of DS resource record registered in the root zone with the one corresponding to re-generated KSK.

When the ZSK is compromised, TWNI carries out the following procedures:
- Re-generation of ZSK.
- Composition of signature for DNSKEY resource records containing re-generated ZSK by KSK.
- Composition of signatures for authoritative records by re-generated ZSK.

4.5.4. Business continuity and IT disaster recovery capabilities

TWNIC will practice business continuity plan testing at least once a year. The testing including any critical system of SRS such as database, EPP and DNS… etc and the operation required elements such as office, facility and human resource.

Follow up the risk assessment and management procedures of the information assets, to ensure the availability, integrity and confidentiality of the information assets.

The key policy objectives of the plan are:

- Provide for the safety, security, and well-being of people on the premises at the time of a disaster;
- Continue critical business operations and ensure continuation of services to TWNIC's customers;
- Limit the duration of a serious disruption to operations and resources (both information processing and other resources) to two business days or less, and minimize the risk of delay in setting up alternate business location;
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective coordination of recovery tasks;
- Reduce the complexity of the recovery effort by minimizing the decision-making processes required during disaster recovery; and
- Identify critical and supporting functions.

4.6. Entity Termination

TWNIC has adopted a DNSSEC termination plan in the event that the roles and responsibilities of the 政府 Zone ZSK and KSK Operator must transition to other entities. TWNIC will co-ordinate with all required parties 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

The key pair generation with the following characteristics:

- In TWNIC private network, it is protected by firewall.
- No remote login, only console access.
- Direct access to HSM in private network and access to registry DB via VPN.
- Dual replicated servers in TWNIC data center.

5.1.2. Public key delivery

TWNIC deploys KSK public key and ZSK private/public key into DNSSEC Service System by using the Encryption Media. KSK public key is not distributed to relying parties in any other way of DNS protocols.

5.1.3. Public key parameters generation and quality checking

TWNIC 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 KSK & ZSK private key will be used only for signing the relevant 政府 zones' RRsets or self-signing its own DNSKEY RR sets to provide proof of possession of private key.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic module standards and controls

TWNIC uses hardware security module for key pair generation and private key storage.

5.2.2. Private key multi-person control

Operations using KSK private key are performed by multiple Trusted Persons.

5.2.3. Private key escrow

Private keys are not escrowed.

5.2.4. Private key backup

For disaster recovery purposes, TWNIC backups KSK private key into separate cryptographic modules. These cryptographic modules are stored in lockable cabinets at two different locations.

5.2.5. Private key storage on cryptographic module

Private keys held on hardware cryptographic modules are stored in encrypted form.

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

Once private key is installed in the cryptographic module, it cannot be retrieved. In case of using private key installed in the cryptographic module, operation by multiple Trusted Persons is required.

5.2.8. Method of activating private key

For the activation of a private key some specific activation data must be entered in the cryptographic module. At least the activation data must consist in a PIN or passphrase.

5.2.9. Method of deactivating private key

No need to deactivate private key.

5.2.10. Method of destroying private key

KSK/ZSK private keys are destroyed when they are expired. Trusted Persons will issue delete command to HSM.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

ZSK and KSK public keys are backed up and archived as part of TWNIC routine backup procedures.

5.3.2. Key usage periods

KSK is one year and ZSK is one month.

5.4. Activation Data

5.4.1. Activation data generation and installation

Pass phrases or PINs must be selected while key pair generation.

5.4.2. Activation data protection

TWNIC protects activation data in a sufficiently secure manner.

5.4.3. Other aspects of activation data

No stipulation

5.5. Computer Security Controls

Access to the system will be controlled. Login name and password will not be recorded on the server. Only when providing correct login name and password, the system will start to check and verify the logon. The system will not notify which part is correct or wrong in a failed logon. The number and time of logons will be limited.

5.6. Network Security Controls

Connect and access to DNSSEC system must via authorized network. The network system should be protected by the firewalls to reduce the security risk.

5.7. Timestamping

DNSSEC system synchronizes the system clocks with internal time server with network time protocol, the timestamp is for audit logs and inception/expiration time for validity period of RRSIG.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

Any software updates on production system are following ISMS procedures to do version control, test and deploy.

5.8.2. Security management controls

TWNIC operates an Information Security Management System/Quality Management System which complies with the requirement of ISO/IEC 27001:2005/ISO 9001:2008 respectively, for the DNS resolution service and domain name registration system.

5.8.3. Life cycle security controls

No stipulation.

6. ZONE SIGNING

6.1. Key Lengths, Key Types, and Algorithms

KSK digest algorithm: RSA/SHA256 (RFC 5702)
KSK size: 2048bits (RFC 4641 section 3.5)
KSK rollover: every year
ZSK digest algorithm: RSA/SHA256 (RFC 5702)
ZSK size: 1024bits
ZSK rollover: every month
Authenticated Denial of Existence: NSEC3 (RFC 5155)
DS digest Type: SHA256 (RFC 4509)

6.2. Authenticated Denial of Existence

TWNIC use NSEC3 resource records with Opt-Out flag specified in RFC 5155.

6.3. Signature Format

The signature format for resource records is RSA/SHA-2 specified in RFC 5702.

6.4. Zone Signing Key Rollover

Every one month.

6.5. Key Signing Key Rollover

Every one year.

6.6. Signature Validity Period and Re-signing Frequency

Re-signing frequencies for KSK and ZSK are per month and per week.

6.7. Verification of Resource Records

TWNIC verifies that all the resource records are conformant with the protocol standards before they are published.

6.7. Resource Records TTL

DS: 86400
NSEC3: 900
DNSKEY: 86400
RRSIG: same as the covered RR

7. COMPLIANCE AUDIT

Compliance audits are included in ISMS (ISO27001) audit.

7.1. Frequency of entity compliance audit

Compliance audits are conducted annually which include internal and external audits.

7.2. Identity/qualifications of auditor

The internal compliance audits are performed by technical staffs with DNSSEC experiences and ISMS lead auditor license, the external audits are performed by BSI Taiwan. They shall be able to demonstrate proficiency in information security auditing, security, DNS and DNSSEC.

7.3. Auditor's relationship to audited party

For external audits, BSI appoints independent auditors to conduct the audits, the auditors may engage TWNIC’s ISMS lead auditor to perform the audit.

7.4. Topics covered by audit

The scope of annual compliance audit includes all DNSSEC implement and operations such as security police, access control, access privilege, key management, software and hardware security, log and backup and key life cycle management.

7.5. Actions taken as a result of deficiency

Any deficiencies found during the internal and external audits will go into correction and prevention process by ISMS team in TWNIC, an appropriate correction plan will be developed and implemented.

7.6. Communication of results

The results of the audits shall be send to BSI for certificate. The auditing reports are not made public.

8. LEGAL MATTERS

8.1 Fee

For registrars there is no extra fee for any function related to DNSSEC.

8.2 Financial responsibility

TWNIC 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 log and reports
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of TWNIC hardware and software and the administration of DNS Keys

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 TWNIC and will not be subject to access restriction.

8.3.3. Responsibility to protect confidential information

TWNIC 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

TWNIC shall be entitled to disclose Confidential/Private Information if, in good faith, TWNIC 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

TWNIC 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 TWNIC'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 TWNIC repository. Amendments to this DPS become effective upon publication in TWNIC 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 Taiwan.