ABC
DNSSEC Practice Statement (DPS)

Most recently saved: 6 June 2012

This document states the Domain Name System Security Extensions policies and practices in effect in ABC's Registry operations. It describes the practices and provisions that ABC employs in providing key management and zone signing services.

Document Control

Document Information and Security

Conducted By	Responsible For Facts	Responsible For Document
Chief Security Officer	Chief Security Officer	Chief Security Officer

Security Classification	File Name
Open	ABC_DPS.doc

Approved by

Date	Name	Function
16 Dec 2010	Bert	Chief Security Officer
8 Sep 2011	Kathie	Chief Information Officer
12 Sep 2011	Kathie	Chief Information Officer

Audits

Date	Version	Name	Description
16 Dec 2010	1.0	BK	Policy and Practice Statement (DPS)
7 Feb 2011	1.0	KW	Internal Consultation Round
1 Apr 2011	1.0	KW	Minor edit
15 July 2011	1.1	KW	Correction of translation mistakes
3 Aug 2011	1.1	RL	Remarks from EDG
8 Sep 2011	1.1	RL	Final version
12 Sep 2011	1.1	RL	Updates due to changes in ABC policy
18 Apr 2012	1.2	RL	Modified for MENOG 10 training
6 Jun 2012	1.3	RL	Modified for CaribNOG 3 training

Contents

1 Introduction

This document (this "DPS") is ABC's statement of security practices that are applied to its DNS Security Extensions (DNSSEC) operations. This document conforms with RFC-draft Framework for DNSSEC Policies and DNSSEC Practice Statements, version 8, at the time this DPS was last revised. The DPS is one of several documents relevant to the operation of the ABC zone. Other relevant documents are ABC's baseline security standard, ABC's information security policy and ABC's business contingency plan. In some cases, these documents, which may be non-public information (for internal use only), are referenced.

1.1 Overview

DNSSEC is a set of records and protocol modifications that provide authentication of the signer of the DNS data, verification of integrity of the DNS data against modification, non-repudiation of DNS data that have been signed, and authenticated denial of existence of DNS records. DNS data secured with DNSSEC are cryptographically signed and incorporate asymmetric cryptography in the DNS hierarchy, whereby trust follows the same chain as the DNS tree, meaning that trust originates from the root and is delegated in the same way as the control of a domain. DNSSEC does not enhance the availability of DNS data, nor does it provide any form of confidentiality.

The DPS is only one of a set of documents relevant to ABC's DNSSEC operations. Other documents include ancillary security and operational documents that supplement the DPS by providing more detailed requirements, such as the Key Ceremony Reference Guide, which presents detailed key management operational procedures. In some instances, where including the specifics are not relevant to the purpose of the DPS, the DPS refers to these ancillary documents for specific, detailed practices implementing ABC policies.

1.2 Document name and identification

Document title: Practice Statement (DPS)
Version: 1.3
Created: 15 July 2011
Updated: 6 Jun 2012

1.3 Community and applicability

Roles and delegation of liability are as follows. The relation between the Registry and a Registrar is regulated in the Registry-Registrar Agreement which may be found as a whole at http://www.ABC.

1.3.1 Registry

ABC (ABC Incorporated) bears responsibility for the domain ABC. ABC administers domain names that identify underlying zones in the ABC zone. This means that ABC manages all data that are related to a domain name.

The registry is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys. The registry is also responsible for securely signing all authoritative DNS resource records in the ABC zone.

Finally, the registry is responsible for the secure export and publication of trust anchors (TA) and the registration and maintenance of DS resource records in the parent zone.

1.3.2 Registrars

A Registrar is the party that is responsible for the administration and management of domain names of behalf of Registrants. The Registrar handles the registration, maintenance and management of a Registrant's domain name and is accredited by ABC.

The Registrar is responsible for securely identifying 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 Registrants

A Registrant is the physical or legal entity that enjoys beneficial control over a domain name. Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the Registrar.

Registrants are responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

1.3.4 Relying party

A Relying Party is the entity that relies on DNSSEC, such as security-aware validating resolvers and other applications that perform validation of DNSSEC signatures. The Relying Party must properly configure and update the Trust Anchors as appropriate. Relying Parties must also stay informed of any relevant DNSSEC-related events in the ABC domain.

1.3.5 Applicability

Each Registrant is responsible for determining the relevant level of security for their domain. This DPS is exclusively applicable to the ABC domain and describes the procedures and security controls and practices applicable when managing and employing keys and signatures for ABC's signing of the ABC zone.

With the support of this DPS, the Relying Party must evaluate its own environment and its associated threats and vulnerabilities to determine the level of trust it may assign to DNSSEC in the ABC domain and the level of risk it is willing to accept.

1.4 Specification administration

This DPS may be updated from time to time by the ABC DNSSEC Policy Management Authority (PMA), including, without limitation, revisions that reflect modifications in systems or procedures that affect the content of this DPS or ABC DNSSEC operations. The PMA is responsible for the

management of the DPS and should be considered the point of contact for all matters related to the DPS.

1.4.1 Document Management

ABC Incorporated
PO Box 19036
Millbrae, California 94030 USA

1.4.2 Contact information

DNSSEC Policy Management Authority
ABC Incorporated
PO Box 19036
Millbrae, California 94030 USA
Telephone: +1 202 709 5262
Fax: +1 707 885 1704
Corp. Reg. No.: 20-04712337
https://www.ABC
dnssec-pma@ABC

1.4.3 Specification change procedures

Amendments to this DPS are made by the ABC DNSSEC PMA. Amendments are either made in the form of amendments to the existing document or published in a new version of the document. This DPS and any amendments to it are published at https://www.ABC/dnssec.

Only the most recent version of this DPS is applicable and any amendments to it, as published by ABC, are applicable. ABC reserves the right to amend or restate the DPS and any amendments to it from time to time without prior notification. Any changes are effective immediately upon publication by ABC. The decision to designate amendments as material or non-material is within the PMA's sole discretion.

2 Publication and Repositories

2.1 Publication site

ABC publishes DNSSEC-relevant information on ABC's website at https://www.ABC/dnssec. The electronic version of this DPS at this specific address is the official version. Notifications relevant to DNSSEC in ABC are distributed by e-mail originating from dnssec-announce@lists.ABC.

2.2 Publication of key signing keys (KSK)

ABC publishes KSKs in the form of a DNSKEY and DS as follows:

- ABC's website, https://www.ABC/dnssec/public-key-for-dnssec/
- Directly in the parent zone (only DS)

The public part of ABC's KSK may be signed with its official PGP-key.

2.3 Access control

Information concerning DNSSEC published at https://www.ABC/dnssec is available to the general public.

3 Operational Requirements

3.1 Meaning of domain names

A domain name is a unique identifier, which is often associated with services such as web hosting or e-mail. Application for registry under the ABC domain is open to all physical and legal entities that have a civil or corporate registration number or that can be identified through the registry list in registers recorded by an authority or an organization with a designation similar to that of an authority. The “first come, first serve” approach applies to the new registration of domain names, meaning that domain names are allocated in the order in which the applications are received by the ABC registry.

In other words, there does not need to be a correlation between the domain name and the Registrant of that domain.

3.2 Activation of DNSSEC for child zone

DNSSEC is activated by at least one DS record for the zone being sent from the Registrar to the Registry and thus being published in the DNS, which established a chain of trust to the child zone. The Registry presumes that the DS record is correct and will not perform any specific controls.

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 contract between ABC and the Registrar.

3.4 Registration of delegation signer (DS) records

The Registry accepts DS records through the EPP interface from each Registrar. The DS record must be valid and sent in the format indicated in RFC 4310 (EPP DNS Security Extensions Mapping). Up to six DS records can be registered per domain name.

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 or those deemed necessary.

3.6 Removal of DS record

A DS record is deregistered via a deletion request passed from the Registrant to the Registrar to the Registry. Deregistration of all DS records associated with a child zone deactivates the DNSSEC security mechanism for that child zone.

3.6.1 Authority to request deregistration

Only the Registrant, or the party formally designated by the Registrant by assigning either the Tech C or Admin C role, has the authority to request deregistration of the DS records.

3.6.2 Deregistration procedure

The Registrant or the Registrant's representative in the form of Tech C or Admin C tasks the Registrar with implementing deregistration. The Registrar may only do this on behalf of the Registrant. From the time deregistration request has been received by ABC via EPP, it takes no longer than until the next zone generation for the change to be recorded in the zone file. Subsequently, it takes up to two times the TTL plus the distribution time before the changes have been deployed. The whole procedure may take a maximum of five hours to complete.

3.6.3 Emergency procedure for deregistration

If a Registrant finds himself in a situation in which he is unable to reach the Registrar, ABC can deregister the DS record, provided the Registrant can be securely identified.

4 Facility, Management, and Operational Controls

4.1 Physical controls

ABC has implemented physical security controls to meet the requirements specified in this DPS.

4.1.1 Site location and construction

ABC has established two fully operational and geographically dispersed operation centers – one primary and one backup - at least 5 kilometers apart. The backup facility contains a complete set of the Registry's critical systems, whose information is continuously updated through automatic replication of the primary operations facility. All of the system components are protected within a physical perimeter with an access control and alarm system operated by ABC.

The backup operations facility meets the minimum standards applied to the primary facility in terms of physical security, power supply, environment and fire and water protection.

4.1.2 Physical access

Physical access to the protected environment is limited to authorized personnel. All entry is logged and the environment continuously monitored.

4.1.3 Power and air conditioning

Power is provided to the operational facilities through several separate sources. In the event of power outages, power is provided by UPS until the backup power systems have begun to generate electricity. The backup power systems have the capacity to supply critical resources with electricity for at least four days.

4.1.4 Water exposures

The facilities implement flooding protection and detection mechanisms.

4.1.5 Fire prevention and protection

The facilities are equipped with fire detection and extinguishing systems. The facilities are equipped with automatic extinguishers with dry extinguishing and fireproof floors. Each room constitutes an independent fire cell.

4.1.6 Media storage

The Registry's guidelines for information classification define the requirements imposed for the storage of sensitive data.

4.1.7 Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, either by the Registry or by a contracted party.

4.1.8 Offsite backup

Certain critical data is also securely stored using a third-party storage facility. Physical access to the storage facility is limited to authorized personnel. The storage facility is geographically and administratively separated from ABC's other facilities.

4.2 Procedural controls

4.2.1 Trusted roles

Trusted roles are held by persons who are able to affect the zone file's content, delivery of trust anchors or generation or use of private keys. The trusted roles are:

1. Systems Administrator, SA
2. Security Officer, SO
3. Safe Controller, SC

4.2.2 Number of persons required per task

At any given time, as backup, there must be at least two individuals within the organization per trusted role indicated in 4.2.1.

HSM activation requires three people to be present; one from each role.

Key generation requires three people to be present; one from each role.

The export and control of trust anchors requires three people to be present; one from each role.

None of the aforementioned operations may be performed in the presence of unauthorized people.

4.2.3 Identification and authentication for each role

Only people who have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with the Registry may hold a trusted role. Before a person receives his or her credentials for system access, a valid form of identification must be presented. Refer to 4.3.2.

4.2.4 Separation of duties

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

4.2.5 Other authorized persons

Other authorized persons include:

- Internal Witness, IW
- External Witness, EW
- Ceremony Administrator, CA
- Master of Ceremonies, MC

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must be able to present proof of the requisite background and qualifications.

4.3.2 Background check procedures

The evaluation of background checks is conducted by the Human Resources (HR) function at ABC. The control of backgrounds and qualifications includes reviewing

- The candidates resume,
- Previous employments,
- References (unclassified and others),
- Documentation confirming the relevant and completed education,
- Financial position through a credit check.

To qualify for any of the trusted roles, these controls cannot reveal any discrepancies that indicate unsuitability as determined by ABC.

4.3.3 Training requirements

The Registry provides the relevant and requisite training regarding procedures, administration and technical systems associated with each trusted role. Training includes:

- ABC's operations
- The role's scope, areas of responsibility and authority.
- Concept of structural separation of roles and access
- Basic technical proficiency in DNS and DNSSEC (for SO and SC)
- Advanced technical proficiency in DNS and DNSSEC (for SA)
- Basic knowledge of information security
- Administration, procedures and checklists.
- Procedures for incident management
- Procedures for crisis management.

The trusted role holder's knowledge is evaluated by ABC's Human Resources function.

4.3.4 Retraining frequency and requirements

People holding trusted roles are subject to continuous evaluation and may be required to undertake supplementary training periodically or in the event of major changes, as determined by ABC.

4.3.5 Job rotation frequency and sequence

Specific operational responsibilities are rotated on occasion, at ABC's sole discretion, among the people who hold trusted roles. ABC may replace any trusted person at any time.

4.3.6 Response to unauthorized actions

Disciplinary actions resulting from unauthorized activities are regulated in the responsibility agreement. Severe negligence may lead to termination and liability for damages.

4.3.7 Contracting personnel requirements

In certain circumstances, ABC may need to use contractors as a supplement to full-time employees. These contractors sign the same responsibility agreements as full-time employees. Contractors who have not been subject to a background check and training, and thus are not qualified for a trusted role, may not participate in the activities indicated in 4.2.2.

4.3.8 Documentation supplied to personnel

ABC Registry IT operations supply the documentation necessary for all personnel to perform their work task in a secure and satisfactory manner.

4.4 Audit logging procedures

Information regarding the activities that take place and the operational status and security state of the system are automatically and continuously collected. This log information is used in monitoring the performance, availability, and correct operation of the system, for statistical purposes, and for investigation of suspected violations of ABC's policies, procedures, or regulations.

In addition to automatically collected sensor and process-status information, logs also include journals, checklists, and other documents that may be required to reconstruct a complete picture of the state of the system or a timeline of events.

The ultimate goal of logging is to enable investigating auditors to completely understand and attribute any failures that may occur, after the fact. To that end, log information identifies individuals, components, and processes and provides as much information as possible about what occurred, when, and for what purpose.

4.4.1 Types of events recorded

The following events are included in logging:

- All types of activities that involve HSM, such as key generation, key activation, and signing and exporting keys.
- Remote access, successful and unsuccessful.
- Privileged operations.
- Entry to a facility or access to equipment.

- Sensor input that indicates activity or a change of state.

Sensor input that indicates inactivity or continuity of state may be published in real time but may, at ABC's discretion, be elided from the long-term archive.

4.4.2 Frequency of processing log

Logs are continuously analyzed through automated and manual controls. Specific controls are conducted on processes including key generation, system reboots and detected anomalies.

4.4.3 Retention period for audit log information

Log information is archived for not less than ten years.

4.4.4 Protection of audit log

All electronic log information is stored in at least two ABC facilities. The logging system is protected against unauthorized viewing and manipulation of information.

4.4.5 Audit log backup procedures

All electronic log information is securely backed up and is stored separately from the system in a secure location. All paper-based log information is scanned and electronically transferred to at least two ABC facilities.

4.4.6 Audit collection system

Electronic log information is transferred via a collection system external to the key-generating system. Manual logs are recorded on paper, scanned, and manually transferred to the collection system. The original documents are archived in a fireproof safe.

4.4.7 Notification to event-causing entity

Notification is hereby given that logging is taking place. No notice is required to be given to any individual, organization, device, or application causing or appearing in a log event, nor does any such party have any special entitlement to view logs.

4.4.8 Vulnerability assessments

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

4.5 Compromise and disaster recovery

4.5.1 Incident and compromise handling procedures

All real and perceived security events that cause or could compromise the integrity of the DNSSEC system or cause disruption of or defects in the service are defined as incidents.

Incidents are handled in accordance with ABC's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, identifying any effects of the incident, and evaluating measures to prevent the incident from recurring.

In the event that any private key is reasonably suspected of compromise or misuse, that key is immediately rolled pursuant to the procedures described in Section 4.5.3.

4.5.2 Corrupted computing resources, software, or data

In the event of corruption, the incident management procedures are initiated and appropriate measures taken as defined in this DPS.

4.5.3 Entity private key compromise procedures

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:

- If a zone signing key is suspected of being compromised, a new ZSK and signed DNSKEY RRsets are generated. The old key will be scheduled for removal from the key set as soon as possible (e.g. sufficient time passes for caches to expire). If a ZSK is suspected of having been compromised or revealed to unauthorized parties, this will be notified through the channels indicated in 2.1.
- If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents. A KSK rollover in progress is always notified through the channels indicated in 2.1.
- If a KSK is lost, a new KSK will be immediately generated and new signed DNSKEY RRsets created starting with the current ZSK. The new KSK's associated DS record is submitted to IANA as an emergency request to add to the current DS set. As soon as it has been published and propagated through caches, ABC starts using the new DNSKEY RRsets. At such time, that will be announced through the channels indicated in 2.1. Relying parties with a static configuration of ABC's trust-anchor should add the new KSK as an extra trust-anchor, in advance. During the time until the rollover, the key set will remain static and any scheduled ZSK rollover will be postponed until after the KSK switch.

4.5.4 Business continuity and IT disaster recovery capabilities

The Registry contingency plan ensures that operation-critical production can be relocated between the two operational facilities within four hours. The facilities are equivalent in terms of physical and logistical protection. Information is replicated between the facilities. Frequently used spare components and critical hardware components are stored onsite in each operation's facility.

The contingency plan and routines are tested regularly. The completed tests and trials are recorded and subsequently evaluated.

The contingency plan includes:

- Who decides on the activation of an emergency recovery procedure.
- How and where the crisis management shall convene.
- Activation of backup operations.
- Activation of public communication plan

- Appointment of a Task Manager.
- Criteria for restoring normal operations.

4.5.5 Entity termination

If the Registry must discontinue DNSSEC for the ABC zone for any reason and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed. If operations are to be transferred to another party, the Registry will participate in the transition so as to make it as smooth as possible.

5 Technical Security Controls

5.1 Key pair generation and installation

5.1.1 Key pair generation

Key generation takes place in an off-line, diskless laptop using a hardware based random number generator.

The resultant key signing key is stored in multiple smartcard based hardware security modules (HSM) that are managed by trained and specifically appointed personnel in trusted roles.

The resultant zone signing keys are encrypted and stored on removable media in tamper-evident packaging for transfer to and installation on off-net signer.

Key generation takes place when necessary and must be performed by three people (SA, SC, SO) working in unison. These people are present during the entire operation.

The entire key-generation procedure is logged and video recorded, part of which is done electronically and part of which is done manually on paper by the Internal Witness (IW).

5.1.2 Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SO and SA. The SO is responsible for publishing the public component of the KSK in a secure manner as per 2.2. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3 Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system. A signature created by a DNSSEC key for either a ZSK or a KSK has a maximum validity period of 15 days and signatures are refreshed at least 5 days prior to expiry.

5.2 Private key protection and cryptographic modules engineering controls

KSK and ZSK key generation is performed on an off-line, diskless laptop and hardware random number generator.

The resultant KSK private key is imported onto multiple FIPS 140-2 smartcard based HSMs. The private key is subsequently destroyed.

After generation, all KSK cryptographic signing operations are performed in the smartcard HSM and no private keys are ever found unprotected outside smartcard.

After ZSK key generation, ZSK cryptographic signing operations are performed using the software based private key in a physically and logically protected off-net server acting as a bump-in-the-wire signer.

5.2.1 Cryptographic module standards and controls

The system uses a smartcard HSM conforming to FIPS 140-2 level 3 requirements (via PKCS11 interface) for KSK and ZSK random number generation, KSK storage and signing operations. ZSK operations employ OpenSSL and BIND software.

5.2.2 Private key (m-of-n) multi-person control

A SO is required to activate the module, which in turn requires physical access, which can only be performed by the SA and SC together.

5.2.3 Private key escrow

The Registry does not utilize a key escrow.

5.2.4 Private key backup

KSKs are stored in un-extractable form in three smartcard HSMs in tamper evident packaging securely stored inside the safes at each operations facility. ZSKs are stored and synchronized between sites in encrypted form after generation.

5.2.5 Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

5.2.6 Method for activating private key

Private keys are activated by unlocking the smartcard HSM. An SA and SC provide an SO with access to the HSM. The SO enters a PIN for the smartcard HSM through a console.

5.2.7 Method of deactivating private key

The smartcard HSM is locked if it is removed from the reader or the system is either turned off or rebooted.

5.2.8 Method of destroying private key

Private keys are not destroyed. After their useful life, they are removed from the signing system.

5.3 Other aspects of key pair management

5.3.1 Public key archival

Public keys are archived in accordance with the archiving of other information relevant to traceability in the system, such as log data.

5.3.2 Key usage periods

Keys become invalid as they are taken out of production. Old keys are not reused.

5.4 Activation data

Activation data is in the form of a SO controlled PIN used to activate the smartcard HSM.

5.4.1 Activation data generation and installation

Each SO is responsible for creating their own activation data pursuant to the applicable requirements of eight characters of varying nature.

5.4.2 Protection of activation data

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

5.5 Computer security controls

All critical components of the Registry's systems are placed in the organization's secure facilities in accordance with 4.1. Access to server operating systems is limited to individuals that require this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

5.6 Network security controls

The Registry has logically sectioned networks that are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. All sensitive information that is transferred over the communications network is always protected by strong encryption.

5.7 Time stamping

ABC retrieves time that is traceable to timeservers from the United States National Institute of Standards and Technology. Time stamps are recorded in UTC and are standardized for all log information and validity time for signatures.

5.8 Life cycle technical controls

5.8.1 System development controls

All source code is stored in a version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe.

ABC's development model is based on industry standards and includes:

- Fully functional specification and documented security requirements,
- Documented architectural design based on a natural modularization of the system,
- Continuous pursuit of minimizing complexity,
- Systematic and automated testing and regression tests,
- Issuing of distinct software versions,
- Constant quality follow-ups of detected defects.

5.8.2 Security management controls

Authorization logs are kept and followed up regularly. The Registry also conducts regular security audits of the system. The Registry prepares and maintains a system security plan that is based on recurring risk analysis.

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 are applied after formal testing and approval. The origin of all software and firmware is securely authenticated by available means.

Critical hardware components of the signer system are procured directly from the manufacturer and transported in tamper-evident packaging to their destination in the secure facility. All hardware is decommissioned within its specified life expectancy.

6 Zone Signing

6.1 Key lengths and algorithms

Key lengths and algorithms are to be of sufficient length for their designated purpose during each key's useful life.

Algorithms shall be standardized by the IETF, available to the public and resource efficient for all parties involved.

The RSA algorithm with a key length of 2048 bits is currently used for KSK and 1024 bits for ZSK.

6.2 Authenticated denial of existence

The Registry uses opt-out NSEC3 records as specified by RFC 5155.

6.3 Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA256.

6.4 Zone signing key rollover (ZSK)

ZSK rollover is carried out every 90-91 days.

6.5 Key signing key rollover (KSK)

KSK rollover is carried out as needed.

6.6 Signature lifetime and resigning frequency

RR sets are signed with ZSKs with a validity period of 15 days. Resigning takes place at least every 10 days. KSK signatures are updated every 10 days according to a pre-defined schedule.

6.7 Verification of zone signing key set

To ensure signatures and the validity period of keys, checks are conducted against the DNSKEY prior to publishing zone information on the Internet.

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 (TTL)

DNSKEY = 3,600 seconds. SOA = 172,800 seconds (2 days). RRSIG inherits TTL from the RR set that it signs.

7 Compliance Audit

Audited documents (policy, procedures, and requirements) and any other relevant, verifiable information can be used in an audit.

7.1 Frequency of entity compliance audit

The need of audits is decided by ABC. Circumstances which may entail an audit requirement are:

- Recurring anomalies.
- Significant changes that are made at the management level, in the organization or in processes.
- Other circumstances, such as the competence among personnel, new equipment or other major changes.

7.2 Identity/qualifications of auditor

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

7.3 Auditor's relationship to the audited party

An external auditing manager is appointed for the audit. When necessary, the auditing manager shall be able to recruit specific expert knowledge. The auditing manager is responsible for implementation during the entire audit.

7.4 Topics covered by audit

The auditing manager's assignment includes ensuring the following:

- ABC possesses the appropriate competencies.
- Auditees are informed of the topic of the audit and prepared prior to the audit.
- Follow-up procedures of the audit results are in place

7.5 Actions taken as result of deficiency

The auditing manager immediately informs ABC management of any anomalies.

7.6 Communication of results

The auditing manager submits a written report of the audit results to ABC management not later than 30 calendar days after completion of the audit.

8 Legal Matters

8.1 Fees

ABC Registry currently does not charge any fees for DNSSEC from Registrars.

8.2 Privacy of personal information

Personal information will be treated in accordance with the US Personal Data Privacy and Security Act and pursuant to other agreements.

8.2.1 Responsibility to Protect Personal Information

This is regulated by ABC's Registration terms and conditions and by agreement between Registry and Registrar.

8.2.2 DISCLOSURE OF PERSONAL INFORMATION TO JUDICIAL AUTHORITIES

Decisions regarding the disclosure of personal information to judicial authorities may be made upon direct request. The matter of disclosure is decided case-by-case in accordance with the US Personal Data Privacy and Security Act. Decisions are made by ABC's legal department.

8.3 Limitations of liability

Liability of damage between the Registry and the Registrar is regulated by section 17 of the Registrar agreement.

ABC's liability of damage toward Registrants is regulated by paragraph 10 of ABC's Registration terms and conditions that are applicable to the domain ABC.

---------- OR ----------

ALL SERVICES PROVIDED BY OR ON BEHALF OF ABC UNDER OR IN CONNECTION WITH THIS DPS (COLLECTIVELY, "SERVICES") ARE PROVIDED "AS IS," "WHERE IS" AND "AS AVAILABLE" WITH ALL RISKS AND FAULTS THAT MAY BE ASSOCIATED IN CONNECTION THEREWITH. NOTWITHSTANDING ANYTHING TO THE CONTRARY, ABC MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND WHATSOEVER WITH RESPECT TO ANY SERVICE, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. ANY AND ALL REPRESENTATIONS, WARRANTIES AND COVENANTS ARE HEREBY DISCLAIMED BY ABC AND WAIVED BY EACH PERSON WHO USES, RELIES UPON, OR BENEFITS FROM ANY SERVICE.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, ABC WILL NOT BE RESPONSIBLE OR OTHERWISE LIABLE, WHETHER AT LAW AND/OR IN EQUITY, FOR ANY CLAIMS AND/OR DAMAGES, INCLUDING, WITHOUT LIMITATION, CONSEQUENTIAL, INCIDENTAL, INDIRECT, PUNITIVE, EXEMPLARY, OR SPECIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, LIABILITIES OR DAMAGES RELATING TO LOST PROFITS, LOST DATA, OR LOSS OF GOODWILL) ARISING OUT OF, RELATING TO, OR OTHERWISE IN CONNECTION WITH ANY SERVICE, WHETHER BASED ON CONTRACT, TORT, OR ANY CAUSE OF ACTION WHATSOEVER.

8.4 Term and termination

8.4.1 Validity period

This DPS applies until further notice.

8.4.2 Expiration of validity

This DPS is valid until it is replaced with an updated or new version as stated in section 1.4.3.

8.4.3 Dispute resolution

Any dispute or conflict resulting from this Agreement shall be filed at San Mateo County California court.

8.4.4 Governing law

The laws of the State of California, excluding its conflict-of-laws principles, shall apply to this DPS.

-- END –