PCH DPS

Packet Clearing House DNSSEC Practice Statement

Most recently updated: 24 June 2011

This document states the Domain Name System Security Extensions policies and practices in effect in Packet Clearing House's operations in its role as DNSSEC Zone Operator on behalf of multiple domain registries. It describes the practices and provisions that PCH employs in providing key management and zone signing services.

DNSSEC Policy Management Authority
Packet Clearing House
572-B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California 94129-0920 USA
+1 415 831 3100
https://pch.net/dnssec
dnssec-pma@pch.net

Contents

1 Introduction 1
1.1 Overview 1
1.2 Document name and identification 1
1.3 Community and applicability 1
1.4 Specification administration 2
2 Publication and Repositories 3
2.1 Publication site 3
2.2 Publication of key signing keys 3
2.3 Access control 3
3 Operational Requirements 3
3.1 Meaning of domain names 3
3.2 Activation of DNSSEC for child zone 3
3.3 Identification and authentication of child zone manager 3
3.4 Registration of delegation signer resource records 3
3.5 Method to prove possession of private key 4
3.6 Removal of DS record 4
4 Facility, Management, and Operational Controls 4
4.1 Physical controls 4
4.2 Procedural controls 5
4.3 Personnel controls 6
4.4 Audit logging procedures 7
4.5 Compromise and disaster recovery 8
5 Technical Security Controls 9
5.1 Key pair generation and installation 9
5.2 Private key protection and cryptographic module engineering controls 10
5.3 Other aspects of key pair management 11
5.4 Activation data 11
5.5 Computer security controls 11
5.6 Network security controls 11
5.7 Time-stamping 11
5.8 Life cycle technical controls 12
6 Zone Signing 12
6.1 Key lengths and algorithms 12
6.2 Authenticated denial of existence 12
6.3 Signature format 12
6.4 Zone signing key rollover 12
6.5 Key signing key rollover 13
6.6 Signature lifetime and resigning frequency 13
6.7 Verification of zone signing key set 13
6.8 Verification of resource records 13
6.9 Resource records time-to-live 13
7 Compliance Audit 13
7.1 Frequency of entity compliance audit 13
7.2 Identity/qualifications of auditor 13
7.3 Auditor's relationship to the audited party 13
7.4 Topics covered by audit 13
7.5 Actions taken as result of deficiency 13
7.6 Communication of results 14
8 Legal Matters 14
8.1 Fees 14
8.2 Privacy of personal information 14
8.3 Limitations of liability 14
8.4 Term and termination 14

1 Introduction

This document (this "DPS") is PCH's statement of security practices that are applied to its DNS Security Extensions (DNSSEC) operations. This DPS conforms with the RFC-draft DNSSEC Policy & Practice Statement Framework, version 4, at the time this DPS was last revised. The DPS is one of several documents relevant to PCH DNSSEC operations. Other relevant documents are PCH's baseline security standard, PCH's information security policy, PCH's business contingency plan, and PCH's Memorandum of Understanding, all of which are published under a Creative Commons Attribution-ShareAlike license, pursuant to Section 2.1 of this document. In some cases, PCH may have a Service Agreement or other agreement containing terms and conditions applicable to PCH's DNSSEC operations that applies bilaterally between PCH and a countersignatory and is private, at the countersigner's request. In some cases, these documents are referenced in this DPS.

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 PCH'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 PCH policies.

1.2 Document name and identification

Document title: DNSSEC Practice Statement (DPS)
Created: 3 March 2011 by Richard Lamb
Updated: 22 March 2011 by Michael Lee
Updated: 14 April 2011 by Bill Woodcock
Updated: 24 June 2011 by Bill Woodcock

1.3 Community and applicability

Roles and delegation of liability are as follows.

1.3.1 Registry

Each Registry bears responsibility for its respective domain and administers domain names that identify zones subsidiary to its zone. This means that the Registry manages all data that are related to a domain name. The Registry is also responsible for the publication of trust anchors (TA) and the registration and maintenance of delegation signer (DS) resource records in the parent zone.

PCH in its role as DNSSEC Zone Operator (DZO) is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys (KSKs) and Zone Signing Keys (ZSKs). PCH is also responsible for securely signing all authoritative DNS resource records in the Registry's zone.

1.3.2 Registrars

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

domain name and is accredited by the Registry. 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 their 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 an 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. The automated method described in RFC 5011 may be used. Relying parties must also stay informed of any relevant DNSSEC-related events in the Registry's domain.

1.3.5 Applicability

Each Registrant is responsible for determining the relevant level of security for its domain. This DPS is exclusively applicable to PCH DNSSEC operations and describes the procedures and security controls and practices applicable when managing and employing keys and signatures for PCH's signing of a client Registry's zone.

With the support of this DPS, each 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 its 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 PCH DNSSEC Policy Management Authority (PMA), including, without limitation, revisions that reflect modifications in systems or procedures that affect the content of this DPS or PCH 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 Specification administration organization

Packet Clearing House
572-B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California 94129-0920 USA

1.4.2 Contact information

DNSSEC Policy Management Authority
Packet Clearing House
572-B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California 94129-0920 USA
+1 415 831 3100 main voice
+1 415 831 3101 fax
https://pch.net/dnssec
dnssec-pma@pch.net

1.4.3 Specification change procedures

Amendments to this DPS are made by the PCH 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://pch.net/dnssec. Only the most recent version of this DPS

and any amendments to it, as published by PCH, are applicable. PCH 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 PCH. 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

PCH publishes DNSSEC-relevant information on PCH's website at https://pch.net/dnssec. The electronic version of this DPS at this specific address is the official version. Notifications relevant to PCH DNSSEC operations are distributed by PGP-signed email originating from dnssec-announce@pch.net.

2.2 Publication of key signing keys

Each Registry is responsible for publishing its KSKs in the form of a DNSKEY and DS as follows:

- Registry's website
- Directly in the parent zone (only DS; when available)
- Emergency KSK according to section 4.5.3.

The public part of the Registry's KSK may be signed with its official PGP-key. PCH may publish copies or links to this information, but the Registry's site remains the authoritative source for such information.

2.3 Access control

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

3 Operational Requirements

3.1 Meaning of domain names

A domain name is a unique identifier that is often associated with services such as web hosting or email. As DZO, PCH exercises no control and asserts no policy over the meaning, content, or form of the domain names contained within the zones it operates.

3.2 Activation of DNSSEC for child zone

DNSSEC is activated by at least one DS record for a zone being published within the zone's parent zone, which establishes a chain of trust from the root of the DNS to the child zone. As DZO, PCH presumes that DS records contained in zones provided to it by Registries are correct and does not perform any specific controls. Registries incorporate DS records into unsigned zones supplied to PCH just as they do NS and other resource records.

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 Registry and Registrar. PCH performs no controls over the identity or authenticity of Registrants.

3.4 Registration of delegation signer resource records

DS records may be generated by or on behalf of Registrants and passed from Registrant to Registrar to Registry in any manner defined by the policies and procedures of the relevant entities. PCH accepts those DS records as resource records embedded within the unsigned zones supplied to PCH by Registries.

3.5 Method to prove possession of private key

PCH does not perform any controls with the aim of validating the Registrant as the manager of a private key. The Registry and Registrar are collectively responsible for conducting the controls that are required or 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. The Registry is responsible for removing the corresponding DS record from the zone, prior to passing the zone as a whole to PCH. Deregistration of all DS records associated with a child zone deactivates the DNSSEC security mechanism for that child zone.

4 Facility, Management, and Operational Controls

4.1 Physical controls

PCH implements physical security controls to meet the requirements specified in this DPS.

4.1.1 Site location and construction

PCH has established two fully operational and geographically dispersed online operation centers to house ZSK operations, in Zurich, Switzerland, and San Jose, United States, 9365 kilometers apart. Both facilities contain a complete set of PCH's critical DNSSEC zone-signing systems. PCH has furthermore established two fully operational and geographically dispersed offline operation centers to house KSK operations, in Singapore and San Jose, United States, 13,594 kilometers apart. Both facilities contain a complete set of PCH's critical DNSSEC key-signing systems. In addition, the Singapore site is equipped to act as a fallback ZSK facility in the event that ZSK operations at both Zurich and San Jose are disabled. All system components are protected within a physical perimeter with an access control and alarm system operated by PCH.

In each facility, all cryptographic key material is housed solely within a FIPS 140-2 Level 4 Hardware Security Module (HSM). The HSM, in turn, is protected within a GSA Class-5 IPS Security Container. The IPS is contained within an enclosure meeting the physical specifications of a DCI 6/9 Sensitive Compartmented Information Facility (SCIF), and the SCIF, in turn, is enclosed within a a room that has been hardened against forced or covert entry, and the interior of which is under constant video surveillance and other monitoring. This room, in turn, is housed within a building that meets or is substantively in accord with the Telecommunications Industry Association specification 942 of a Tier-4 datacenter.

4.1.2 Physical access

Physical access to the protected environment is limited to authorized personnel. Specifically, each HSM requires at least three of PCH's seven Crypto Officers to operate. The IPS Security Container may be opened only by one of PCH's three Security Controllers. The SCIF requires two of PCH's three Security Controllers to open. The hardened room requires one of PCH's three Security Controllers to enter, and entry to the datacenter is controlled by the datacenter Facility Operator. At each stage, entry and exit are logged and the environment is continuously monitored.

4.1.3 Power and air conditioning

Power is provided to the operational facilities from separate sources. In the event of utility power outages, power is provided by PCH-controlled batteries until the datacenter's backup power systems have begun to generate electricity. The backup power systems are engineered to supply electricity indefinitely, provided diesel fuel deliveries are maintained.

4.1.4 Water exposures

The three datacenter facilities implement flood protection and detection mechanisms, and PCH operates separate water detection within each SCIF.

4.1.5 Fire prevention and protection

The three datacenter 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

PCH'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 by one of PCH's three Security Controllers.

4.1.8 Offsite backup

Certain critical data are redundantly stored in a secured, third-party storage facility. Physical access to the storage facility is limited to authorized personnel. The storage facility is geographically and administratively separated from PCH'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

- Crypto Officer, CO
- Security Controller, SC

4.2.2 Number of persons required per task

There must be a minimum of three COs and one SC. Under normal circumstances, there are seven COs and three SCs.

HSM activation requires three COs with their assigned credentials and one SC to be present.

Key generation requires three COs with their assigned credentials and one SC to be present.

The export and control of encrypted key material requires the cooperation of three or five COs, depending on the specific operation, and one SC.

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 PCH may hold a trusted role. Before a person receives his or her credentials for system access and upon each exercise of that access a valid form of identification must be presented. Refer to Section 4.3.2.

4.2.4 Tasks requiring separation of duties

The trusted roles in Section 4.2.1 may not be held simultaneously by one and the same person. The separation of duties is enforced by the Crypto Officers not having exclusive physical access to the operational facilities and the Security Controllers not having access to the activation material of the HSM.

4.2.5 Other authorized persons

Other authorized people may include but are not limited to

- Ceremony Administrator, CA
- External Witness, EW
- Facility Operator, FO
- Systems Administrator, SA
- Registry Representatives, R
- Other authorized Witnesses, W

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must present proof of the requisite background and qualifications to PCH's Human Resources function.

4.3.2 Background check procedures

Background checks are conducted by PCH's Human Resources function. The control of backgrounds and qualifications may include, but is not limited to, reviewing

- Candidate's 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 PCH.

4.3.3 Training requirements

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

- PCH operations
- Role's scope, areas of responsibility, and authority
- Concept of structural separation of roles and access
- Basic technical proficiency in DNS and DNSSEC
- 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 PCH'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 PCH.

4.3.5 Job rotation frequency and sequence

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

4.3.6 Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are determined by PCH and may include termination and damage liability.

4.3.7 Contracting personnel requirements

PCH may at its discretion use contractors or volunteers as well as employees. Such parties sign the same type of responsibility agreements and are subject to essentially the same requirements as employees under this DPS, including but not limited to the same background checks and training.

4.3.8 Documentation supplied to personnel

PCH 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 PCH'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 activities that involve an HSM, such as key generation, key activation, signing, and exporting keys
- Remote access to systems, 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 PCH'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. Logs are examined after each key ceremony for significant security and operational events. In addition, PCH reviews its audit logs for suspicious or unusual activity in response to alerts generated on the basis of irregularities and incidents within the DNSSEC systems and their security environment. Audit log processing consists of a review of logs and documentation for all significant events within a context of interest. Audit log reviews include a verification that the log has not been tampered with and an investigation of any alerts or irregularities in the logs. Actions taken on the basis of audit log reviews are also documented.

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 PCH facilities. Logging collection and storage systems are protected against unauthorized access and manipulation of information. Any log data deemed by PCH to be too sensitive for publication may be redacted or protected against unauthorized access, but generally log data are published for public inspection as they become available.

4.4.5 Audit log backup procedures

As it is collected and as network connectivity permits, electronic log information is continuously transferred to at least one separate and secure online location and periodically backed up to two offline long-term archives. All paper log information is periodically scanned and electronically transferred to the online location and periodically backed up to the long-term archives. The offline long-term archives are in fire- and intrusion-resistant safes in separate locations.

4.4.6 Audit collection system

Electronic log information is transferred via a collection system external to the key-generating system. In the event that network connectivity between any logging facility and the online archive is interrupted, each logging facility has sufficient capacity to independently buffer at least seven days of its own activity at normal rates of collection, and this buffer is immediately transferred to the archive upon reestablishment of network connectivity. Manual logs are recorded on paper, scanned, and periodically entered into the collection system. Original paper documents are archived in one of the offline long-term archives.

4.4.7 Notification to event-causing subject

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

Events in the audit process are logged, in part, to monitor system vulnerabilities. Periodic vulnerability assessments are performed manually as part of the audit log review process. PCH may at its discretion share security-related information with relevant parties in order to improve the security of the DNSSEC signing process or Internet security environment.

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 PCH'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

In the event that any private key is reasonably suspected of compromise or misuse, a controlled key rollover is performed as follows:

- If a ZSK is suspected of being compromised, it is immediately removed from production and no longer used. A new ZSK is generated, if need be, and employed immediately. The old key is removed from the key set as soon as its signatures have expired. If a ZSK is suspected of being compromised, an announcement is made using the mechanisms defined in Section 2.
- If a KSK is suspected of being compromised, a new key is generated and put into immediate use, in parallel with the old key. The appropriate Registry is notified, and a coordinated communication plan is instituted, including requesting the IANA to publish the additional DS record corresponding to the new KSK. The old KSK remains in place and is used to sign key sets until such time as it can be considered sufficiently safe to remove. During the time preceding the rollover, the key set remains static and any scheduled ZSK rollover is postponed until the KSK rollover is complete. A KSK rollover in progress is announced using the mechanisms defined in Section 2 in addition to Registry communications.
- If a KSK is lost, a new key is generated with new DS record. The Registry is notified, and a coordinated communication plan is instituted, including requesting IANA to publish the additional DS corresponding to the new KSK. Once IANA changes are propagated, the old KSK is taken out of service and swapped for the new KSK. At such time, the change is announced using the mechanisms defined in Section 2. During the time preceding the rollover, the key set remains static and any scheduled ZSK rollover is postponed until the KSK swap is complete.

4.5.4 Business continuity and IT disaster recovery capabilities

The PCH 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 is to convene
- Activation of backup operations
- Appointment of a Task Manager
- Criteria for restoring normal operations

4.5.5 Entity termination

If the Registry discontinues DNSSEC for its zone for any reason and returns to an unsigned position, this is to take place in an orderly manner (by removing DS records from IANA), with the full cooperation of PCH. If operations are to be transferred to another party, PCH cooperates fully with the transition.

5 Technical Security Controls

5.1 Key pair generation and installation

5.1.1 Key pair generation

Key generation takes place in a hardware security module (HSM) that is managed by trained and specifically appointed personnel in trusted roles.

Key generation takes place when necessary and must be performed by two people working in unison. These people are present during the entire operation.

The entire key-generation procedure is logged, part of which is done electronically and part of which is done manually on paper by the SO.

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 communicating the public component of the KSK in a secure manner to the Registry. The SA is responsible for ensuring that the keys published in Section 2.2 are the same as those that are generated.

5.1.3 Public key parameters generation and quality checking

Key parameters are regulated by PCH's key-signing policies. Quality control includes checking the key length.

5.1.4 Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system. A signature that is created by a DNSSEC key for either a ZSK or a KSK never has a validity period shorter than fifteen days.

5.2 Private key protection and cryptographic module engineering controls

All KSK and ZSK cryptographic operations are performed in the HSM, and no private keys are unprotected outside the HSM.

5.2.1 Cryptographic module standards and controls

The system uses an HSM that conforms to the requirements in FIPS 140-2 level 4 for KSK and ZSK operations.

5.2.2 Private key (m-of-n) multiperson control

PCH applies multiperson control for HSM activation. Multiple SOs are required to activate the module in a three-of-seven scheme, which in turn requires physical access, which can be provided only by one or more SCs.

5.2.3 Private key escrow

PCH does not utilize key escrow.

5.2.4 Private key backup

KSKs are backed up in encrypted form onto a flash drive securely stored in tamper-evident packaging inside safes at each operations facility. ZSKs are similarly backed up in encrypted form onto another flash drive securely stored in tamper-evident packaging inside safes at each operations facility.

5.2.5 Private key storage on cryptographic module

The Storage Master Key (SMK) is shared by all security modules in the system. This master key is used to secure the contents of the HSM and to enable cloning the HSM in case of equipment failure. The SMK is split across seven smartcards held by trusted Internet community members in a five-of-seven scheme. Cards are kept inside tamper-evident packaging and are subject to annual inventory requirements.

5.2.6 Private key archival

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

5.2.7 Private key transfer into or from a cryptographic module

During the installation of the signing system, a joint Storage Master Key is transferred via the above smartcards to clone units. Transfer of KSK and ZSK material between units is done via encrypted backups, as described in Section 5.2.4, which can be decrypted only into initially cloned units. After transfer, ZSK HSMs are locked to prevent further export of keys.

5.2.8 Method of activating private key

Private keys are activated by unlocking the HSM. An SA provides SOs access to the facility. The SOs then each insert their smartcard and enter a PIN.

5.2.9 Method of deactivating private key

The HSM is locked if the signing system is either turned off or rebooted.

5.2.10 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 are in the form of a smartcard and PIN for each SO that are used to activate the HSM.

5.4.1 Activation data generation and installation

SO smartcards are generated during the initialization of the HSMs during the initialization key ceremony.

5.4.2 Activation data protection

Each SO is responsible for protecting his or her smartcard. On the suspicion of compromise, the SO must immediately notify PCH and PCH replaces all SOs smartcards at the next key ceremony. PCH's DNSSEC contingency plan states the conditions in which this is to be applied. All decommissioned smartcards are physically destroyed by SCs in the presence of witnesses.

5.5 Computer security controls

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

5.6 Network security controls

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

5.7 Time-stamping

PCH 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 fire- and intrusion-resistant safe.

PCH'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 minimization of complexity
- Systematic and automated testing and regression tests
- Issuing distinct software versions
- Constant quality follow-ups of detected defects

5.8.2 Security management controls

Authorization registers are maintained. PCH conducts regular security audits of the system. PCH 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 bags 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 KSKs, and 1024 bits for ZSKs.

6.2 Authenticated denial of existence

PCH uses NSEC3 records as specified by RFC 5155, and may sort zones prior to signing, in order to maximize NSEC3 efficiency.

6.3 Signature format

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

6.4 Zone signing key rollover

ZSK rollover varies depending on zone (e.g., SOA and TTL values) but occurs at least once every six months.

6.5 Key signing key rollover

KSK rollover is carried out as needed.

6.6 Signature lifetime and resigning frequency

Resource Record Sets (RRsets) are signed with ZSKs with a validity period depending on zone parameters, but at least seven days.

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 DNSKEY KSK signature and ZSK signature on NS RRset.

6.8 Verification of resource records

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

6.9 Resource records time-to-live

DNSKEY TTL is set to 3600 seconds for all zones. TTL for other records is set by Registry in the unsigned zone file provided to PCH. RRSIG inherits TTL from the RRset 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

PCH determines the need for audits. Circumstances that may initiate an audit include but are not limited to recurring anomalies; significant organizational changes at the management level or in processes; issues of personnel competence; and new equipment.

7.2 Identity/qualifications of auditor

The auditor shall be able to demonstrate an understanding of 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 of the entire audit.

7.4 Topics covered by audit

The auditing manager's assignment includes ensuring the following:

- PCH 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 PCH management of any anomalies.

7.6 Communication of results

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

8 Legal Matters

8.1 Fees

PCH does not charge country-code top-level Domain Administrators any fees for DNSSEC services.

8.2 Privacy of personal information

All information is treated in accordance with the PCH Privacy Policy and the applicable written agreement between the Registry and PCH (the PCH-Registry Agreement). PCH does not receive personally identifiable information about individuals from Registries and thus undertakes no special responsibility with respect to the protection of personally identifiable information. Decisions regarding the disclosure of information to judicial or governmental authorities may be made upon direct request. The matter of disclosure is decided case-by-case by the PCH legal department.

8.3 Limitations of liability

ALL SERVICES PROVIDED BY OR ON BEHALF OF PCH 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, PCH 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 PCH AND WAIVED BY EACH PERSON WHO USES, RELIES UPON, OR BENEFITS FROM ANY SERVICE.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, PCH 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 in connection with this DPS is to be filed in federal or state court, City and County of San Francisco, California.

8.4.4 Governing law

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

– END –