Root Zone KSK Operator Document Management Procedure

Version 3.3

Root Zone KSK Operator Policy Management Authority

22 September 2021

Table of Contents

1 Introduction

Public Technical Identifiers (PTI) performs the Root Zone Key Signing Key (RZ KSK) Operator role pursuant to a contract from the Internet Corporation for Assigned Names and Numbers (ICANN).

The purpose of this procedure is to support managing the life cycle of the documents related to RZ KSK operations. Proper management of the life cycle plays an essential role in mitigating risks of having major/minor audit nonconformities and having a successful annual audit. In case the nonconformity is serious enough, it could cause unfavorable consequences such as audit failure and unexpected expenses to fix the issue. In addition, from a knowledge management perspective, promptly updating documents based on the insights and experiences of the personnel performing the operations will prevent degradation of the service from irreversible loss of knowledge and increase the stability and resilience of the operation.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2 Objective and Scope

There are two main objectives for this document. One is to ensure that the process is properly documented and in compliance with requirements, including regulatory, technical, and governing documents (e.g., policies). The second is to make sure the actual operation reflects what is documented and vice versa so that either the process or the document can be corrected. These two objectives are assessed during the annual third-party audit Service Organization Control 3 (SOC 3) certification.

This document is designed to support the stakeholders involved in the life cycle of document management, especially document owners who need to understand what actions are required to properly manage the documents. Document reviewers and approvers are also supported by this document.

The scope is limited to the documents of the RZ KSK operations, more specifically all documents that fall under the DNSSEC Practice Statement for the Root Zone KSK Operator (DPS).

3 Roles and Responsibilities

This section describes the roles and responsibilities of the personnel involved in the document management process.

3.1 RZ KSK Operator Policy Management Authority

The RZ KSK Operator Policy Management Authority (PMA) is an advisory group responsible for reviewing and approving the DPS and all subsequent policy and procedure documents. The PMA MAY be consulted for assistance in evaluating compliance questions or determining the appropriateness of the proposed change to the documents. Ultimately, all topics that could possibly affect the documents SHOULD be discussed by the PMA, so document owners and other stakeholders are encouraged to actively post questions or concerns to the PMA.

3.2 RZ KSK Operations Security

RZ KSK Operations Security (RKOS) is responsible for security reviews and approvals for policy and procedure documents. RKOS is more focused on performing reviews from a security perspective, and periodically conducts an internal audit to assure the procedures are properly implemented according to the document. In addition, RKOS is responsible for tracking the audit trails for document management. All policy violations are to be reported to RKOS in order to invoke the incident management process.

3.3 Line Manager

The line manager is responsible for reviewing and approving policy and procedure documents. It is also solely the line manager's responsibility to enforce the policy and procedure documents and ensure all discrepancies between document and practice are promptly addressed and remediated. The line manager is also expected to provide the "manager's response" in case nonconformity is discovered during the audit.

3.4 Document Owner

The document owner is in charge of maintaining the document throughout its life cycle. This person MAY or MAY not be the author of the document. The document owner is responsible for implementing the contents of the document and assuring that the document accurately reflects practices. The document owner also initiates the document publication process in case of authoring new documents or making changes to an existing document.

3.5 The Public

There are only certain conditions that require a public review, for example a DPS amendment. Currently, the DPS is the only document REQUIRED to be public facing and open to any questions or suggestions. Disclosure of any other documents related to RZ KSK operation is OPTIONAL and MUST be determined individually.

4 Document Specification

This section lists the types of information REQUIRED for document publication.

4.1 Document Name and Version

All documents MUST have a meaningful document name and version specified within the document. The document name MUST include the document category (policy, procedure, manual, record). The versioning convention is decided by the document owner, but it MUST be consistent within the document.

4.2 Document Categorization

All documents MUST clearly state the document category in order to determine the appropriate publication process. Dual categorization of the document is allowed when a document is carrying enough information to cover both categories.

4.2.1 Policy

A policy is a document that defines the set of principles and rules designed to guide decision making of the organization under certain circumstances. Policies MAY be created for the organization or per topic. Regardless of the granularity, all policy documents MUST be approved by the PMA.

4.2.2 Procedure

A procedure is a document that explains the process operated to accomplish certain objectives. A process converts inputs and produces outputs. The procedure document is designed to provide guidance on what the required input and desired output for a process is by illustrating the relationship between tasks.

4.2.3 Manual

A manual is a document that illustrates the implemented procedures. A manual contains a sequence of activities to complete a specific task. It could be said that a manual is a breakdown of a procedure document that supports performing the task.

4.2.4 Record

A record is a form of information providing evidence or information on past events. Records require reviews but do not require approvals.

4.2.5 Report

A report is a summary of a set of records created under certain circumstances. Reports require reviews but do not require approvals.

4.3 Effective Date

Each document MUST clearly state its effective date. Backdating the effective date is strongly discouraged in order to avoid issues during the annual audit. Setting future dates is allowed upon necessity such as aligning the effective date with the production go-live date.

4.4 Document Owner

A document owner MUST be determined for each document. The document owner MUST be different from the line manager and PMA. The document owner MAY be specified in the document.

4.5 Sensitivity Rating

Each document MUST have a sensitivity rating according to the adopted data classification policy. It is the document owner's responsibility to determine the confidentiality of the document. The confidentiality rating SHOULD be specified in the document when the document contains sensitive information that requires careful handling.

4.6 History of Changes

Policy documents MUST have a history of changes kept either separately or within the document in addition to the evidence of review and approval. Manual and record documents MAY keep the history of changes but MUST keep track of the approval records.

5 Document Publication Process

This section describes the regular process for document publication. The process consists of four steps: proposal, review, approval, and publication. There are two key points in this process. One is to make sure that the document is properly reviewed and approved prior to publication and the record of the discussion during the review and approval is kept for an audit trail. The other is that the impact of changing the document is properly assessed and the governing or subsequent documents are updated accordingly in order to preserve consistency.

5.1 Document Publication Proposal

Prior to submitting the document publication request, the document owner MUST identify the impact of the proposed change on the other related existing documents and record what the ramifications will be. The proposed changes MUST be incorporated into the current version of the document in an unambiguous and self-explanatory manner. Enabling the track changes function of the document processing software is one way to do this. In case the document is in plaintext, a brief description on what the changes are MUST be circulated to the reviewers.

Finally, the document owner kicks off the document publication process by submitting the proposed change or a draft of a new document to the primary reviewer/approver.

5.2 Document Review and Approval

This section introduces the different types of reviews and explains what is expected during a review.

5.2.1 PMA

A PMA review MUST be performed for all policy documents. The PMA reviews the proposed document and confirms the change does not violate the regulatory compliance requirements and is appropriate. This review also serves the purpose of getting management's commitment and reserving the resources necessary to make the changes.

Voting will be performed at the end of the PMA review as described in Root Zone KSK Operator Policy Manager Authority Charter, and the approval will be decided.

An email stating the approval or rejection will be sent out by the PMA Chair designated by the PMA.

5.2.2 Security

A security review MUST be performed by the RKOS for all policy and procedure documents. The purpose of this review is to perform a check from a security perspective to make sure the proposed change does not violate any security and audit requirements.

An email stating the approval or rejection will be sent out by the RKOS. The RKOS also reserves the right to consult the PMA.

5.2.3 Line manager

A line manager review MUST be performed for all manual documents. The line manager checks the feasibility of the change proposal and confirms the necessary resources are provided.

An email stating the approval or rejection will be sent out by the line manager. The line manager reserves the right to consult the PMA. Line manager approval for procedure documents is not when changes are minor or cosmetic.

5.2.4 Public

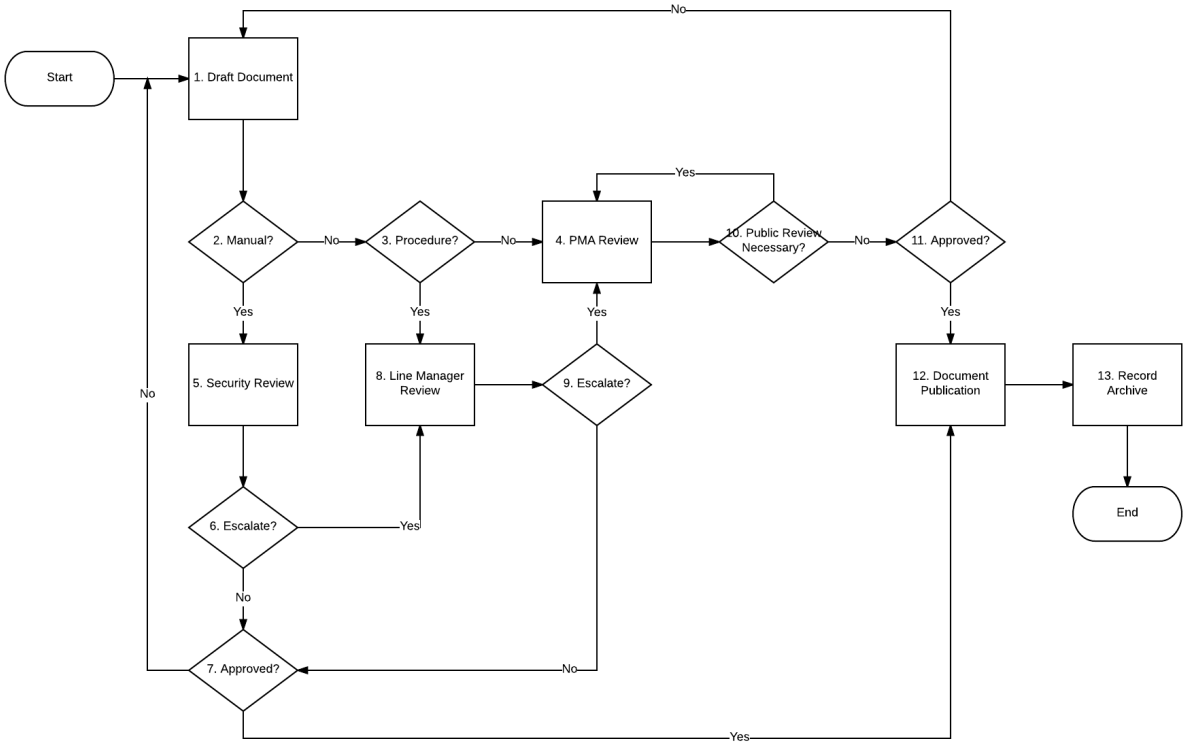
A public review SHOULD be performed for DPS amendments when significant changes are proposed. Exceptional DPS amendments to prevent a breach of security MAY be performed without public review at the discretion of the PMA. Other documents are not subject to public review unless there is a specific reason to do so.

All public reviews are handled by the PMA, more specifically the PMA Chair or other personnel delegated by the PMA. The feedback from the public will be discussed in the PMA.

5.3 Document Publication

Publication is the final step performed after the document is properly reviewed and approved. The record of the review and approval MUST be archived for audit purposes and future reference. The published documents MUST be made available to all stakeholders.

5.4 Document Publication Flow



6 Audit

6.1 Periodic Review

All policy and procedure documents MUST be reviewed at least annually and whenever a significant change is made to RZ KSK operation. The document owner MUST perform the document review and keep a record of it.

6.2 Annual Internal Audit

RKOS MUST perform an internal audit annually to ensure the documents are properly maintained and the processes are effectively implemented on a daily basis. The audit report of the annual audit will be communicated to the PMA.

Appendix A: Acronyms

DPS	DNSSEC Practice Statement for the Root Zone KSK Operator
ICANN	Internet Corporation for Assigned Names and Numbers
KSK	Key Signing Key
PMA	Root Zone KSK Operator Policy Management Authority
PTI	Public Technical Identifiers
RFC	Request for Comments
RKOS	RZ KSK Operations Security
RZ	Root Zone
SOC	Service Organization Control

Appendix B: Change Log

Revision 3 - 04 October 2018

- Converted the document to use the latest Word template.
- Made minor editorial, formatting, and style changes.
- Made all cross-references hyperlinks.
- Adopted the RFC "MUST", "SHOULD", etc. convention throughout each document. Added a paragraph to Section 1 that explains the RFC wording convention.
- Added an acronym list.
- Cover: Changed the version from 2.3 to 3.0.
- Section 1: Wrote an introduction based on previous material from other parts of the document.
- Section 2: Added an Objective and Scope section. Clarified the document's objective and scope.
- Section 3: Condensed text throughout the section to minimize redundancy.
- Section 4.2: Added Section 4.2.5 to define "reports" (moved text from Section 4.2.4).
- Section 4.4: Clarified how the document owner MUST differ from those in other roles.
- Section 6.2: Renamed the section to clarify the purpose and frequency of internal audits.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Updated Appendix A to reflect only the acronyms present in the document.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Made minor grammatical changes.
- Overall: Uniformly specified "Practices Manager" as "PMA Chair".
- Section 4.5: Clarified document sensitivity rating process.
- Section 4.6: Specified "document" as "documents".
- Section 5.2.4: The DPS section 1.4.3 states that DPS amendments can be made if they are going to prevent a breach of security without public review. Updating this document to reflect that scenario, and the standard DPS amendment procedure.

Revision 3.3 - 22 September 2021

- Annual review: Update version information and dates.
- Section 1: Clarified use of key words as described in RFC 2119 and RFC 8174