Root Zone KSK Operator Audit Logging Procedure

Version 3.4

Root Zone KSK Operator Policy Management Authority

19 October 2022

Table of Contents

Introduction **3**

Objective and Scope **3**

Roles and Responsibilities **3**

- Ceremony Administrator 3
- System Administrator 3
- Internal Witness 4
- RZ KSK Operations Security 4

Audit Logging Procedures **4**

- Audit Bundles 4
- Information to Be Collected 5
  - Events Specific to RZ KSK Life Cycle Management 5
  - Events Related to the Signing of Data 5
  - Events Related to Physical Access Control 5
  - Actions Taken as Part of the Incident Handling Process 6
  - Access to Audit Information 6
  - Events Related to Operating System Image Life Cycle Management 6
  - Evidence from Key Ceremony 6
  - Self-assessment and Configuration Review 7

Appendix A: Acronyms **7**

Appendix B: Change Log **8**

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 help ensure that access to Key Management Facilities (KMF) and operations involving the private components of the RZ KSK are recorded, including the parties involved, when they accessed the Key Management Facility (KMF) or RZ KSK, and what operation was performed.

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

The objective for this procedure is to define requirements and recommendations for audit logging procedures to be performed by designated personnel, systems, and other means.

3 Roles and Responsibilities

3.1 Ceremony Administrator

The Ceremony Administrator (CA) designated for a given ceremony is responsible for compiling all audit log information into the audit log information bundle in accordance with section 4.1 of this document.

The CA is also responsible for:

- Collecting and copying the output from the signer system
- Initiating the review of the compiled audit log information bundle by inviting at least one more Trusted Person from another role and jointly reviewing all audit log information

The CA can have access to the offsite storage facility in which audit log materials are stored. Accessing the system logs and access event logs that are stored in the Key Management Facility requires both the Ceremony Administrator and the Internal Witness.

3.2 System Administrator

The System Administrator (SA) is responsible for:

- Collecting and copying the audiovisual recordings from the Key Ceremony

- Providing the event log from the Physical Access Control and Intrusion Detection System (PAC-IDS)
- Performing the self-assessment in accordance with section 4.2.8

The SA MUST assist the CA during the audit log review process and during compilation of the audit bundle.

3.3 Internal Witness

The Internal Witness (IW) MUST assist the CA during the audit log review process and during the compilation of the audit bundle.

3.4 RZ KSK Operations Security

The RZ KSK Operations Security (RKOS) function is responsible for providing copies of all information related to the incident handling process, in accordance with section 4.2.4. The RKOS role MUST have access to the offsite storage facility where audit bundles are stored.

4 Audit Logging Procedures

4.1 Audit Bundles

The audit log information MUST be collected and compiled into audit bundles, consisting of all supporting control evidence documentation for a site, covering a timeframe from the last audit bundle and over a Key Ceremony.

Immediately after each ceremony, the documentation specified in section 4.2 MUST be collected, reviewed, compiled into an audit bundle, and closed. Closing an audit bundle implies having duplicate copies of all collected materials. Both original and copy audit bundles MUST be sealed inside tamper-evident bags. These tamper-evident bags MUST be stored in separate secure locations identified by the RKOS.

The review process MUST include the following:

- Verification of handmade signatures on hard copies
- Verification of the integrity of tamper-evident bags that were sealed in the presence of Trusted Persons

The result of the review and any actions taken as a result of this review MUST be documented, and that documentation MUST be included in the audit bundle.

4.2 Information to Be Collected

The following categories of security-related events MUST be recorded and are considered part of the supporting control evidence documentation.

4.2.1 Events Specific to RZ KSK Life Cycle Management

The following events are critical to the life cycle management of the RZ KSK and MUST be logged:

- Key generation
- Key backup
- Key recovery/installation
- Key activation
- Key usage
- Key destruction

4.2.2 Events Related to the Signing of Data

The signer system MUST validate the Key Signing Request (KSR) by verifying the following:

- Key parameters and algorithms
- Requested signature lifetimes
- Proof-of-possession of private key
- Proof traceable to the last KSR

The signer system MUST log evidence of such verifications, which are to be collected with the rest of the output from the signer system and stored electronically on portable media.

4.2.3 Events Related to Physical Access Control

The PAC-IDS MUST log the following events relevant to the security of the system:

- Assignment, modification, and revocation of access credentials
- Successful and unsuccessful physical access attempts
- Changes in access control privileges
- Intrusion detection or environmental irregularities
- Emergency override of access control
- Other violations of the physical access control policy

This information MAY be exported and stored electronically on portable media or printed and stored as hard copies, whichever is determined to be most convenient by the RKOS. If the information is stored electronically, it MUST be stored in plaintext or Portable Document Format (PDF).

4.2.4 Actions Taken as Part of the Incident Handling Process

The incident handling process MUST be traceable and MUST maintain an audit trail. Incident reports MUST be maintained by RKOS and securely stored with methods preventing their loss or compromise and allowing disclosure upon request. For each reported incident, the following information is to be considered part of the supporting control evidence documentation and MAY be included in the next audit bundle:

- The incident report itself
- The investigation of the incident
- Any actions taken to remedy the effects and/or measures taken to prevent the incident from recurring

4.2.5 Access to Audit Information

Access to any audit information MUST be logged using a log sheet that is stored within the same compartment as the audit bundle itself. At the closing of an audit bundle accessed at a future date, a copy of the log sheet MUST be included.

4.2.6 Events Related to Operating System Image Life Cycle Management

All events relevant to the security of the life cycle management of the operating system image MUST be logged and included as part of the supporting control evidence documentation and included into the audit bundle if such changes have occurred within the timeframe.

To provide this evidence, a report MUST be compiled consisting of:

- The version number of the new software release
- The method used to securely authenticate the operating system image and constituent system software, and the evidence of such validation
- The method and data used to verify that the software on the operating system image originated from the RZ KSK Operator, is the intended version, and has not been modified since the previous Key Ceremony

This report is the supporting control evidence documentation of the operating system image management life cycle and MUST be included in the audit bundle.

4.2.7 Evidence from Key Ceremony

The execution of the Key Ceremony MUST be properly documented by including the following information in the audit bundle:

- The audio/video recording from the ceremony
- The signed ceremony script from physically present attendees

- The IW attestation/affidavit

4.2.8 Self-assessment and Configuration Review

After each Key Ceremony, the following topics are subjects for self-assessment:

- Review of assigned authorizations and roles in the PAC-IDS
- Review of the PAC-IDS configuration for each role
- Review of the PAC-IDS firewall configuration
- Review of the PAC-IDS event log to confirm proper functionality

This review MUST be documented in a report that is part of the supporting control evidence documentation, and MUST be included in the audit bundle.

Appendix A: Acronyms

CA	Ceremony Administrator
ICANN	Internet Corporation for Assigned Names and Numbers
IW	Internal Witness
KMF	Key Management Facility
KSK	Key Signing Key
KSR	Key Signing Request
PAC-IDS	Physical Access Control and Intrusion Detection System
PDF	Portable Document Format
PMA	Root Zone KSK Operator Policy Management Authority
PTI	Public Technical Identifiers
RFC	Request for Comments
RKOS	RZ KSK Operations Security
RZ	Root Zone
SA	System Administrator

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: Added an introductory paragraph. Clarified what types of information are to be recorded.
- Section 2: Added an Objective and Scope section.
- Section 4.2.1: Deleted first sentence because it was redundant.

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 editorial, formatting, and style changes.
- Section 4.2.4: Updated incident report storage procedure.
- Section 4.2.5: Specified that an audit log sheet will only be present in an audit bundle if accessed at a future date after initially sealed.
- Section 4.2.6: Defined “system” as the “operating system image”.
- Section 4.2.8: Replaced “Prior to” with “After” the ceremony for accuracy.

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

Revision 3.4 - 19 October 2022

- Annual review: Update version information and dates.