Root Zone KSK Operator Audit and Accountability Policy

Version 3.2

Root Zone KSK Operator Policy Management Authority

04 November 2020

Table of Contents

Introduction **3**

Objective and Scope **3**

Roles and Responsibilities **3**

- System Administrator 3
- Ceremony Administrator 3
- Internal Witness 4
- Policy Management Authority Chair 4
- RZ KSK Operations Security 4

Security Requirements **4**

- Availability 4
- Integrity 4

Security Controls **4**

- Security Management 4
  - RZ KSK PMA 4
  - RKOS 5
- Types of Events Recorded 5
- Audit Log Collection 5
- Audit Log Reviews 5
- Audit Log Protection 6
- Audit Data Retention 6
- Audit Log Backups 6

Documentation and Accountability **6**

Log and Audit Trail Disclosure **6**

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).

All operations involving the RZ KSK are conducted within physically protected environments called Key Management Facilities (KMF) that deter, prevent, and detect any unauthorized use of, access to, and disclosure of sensitive information and systems, whether covert or overt.

The purpose of this audit and accountability policy is to ensure that any access to Key Management Facilities and any operations involving the private component of the RZ KSK remain traceable in time and to any individual responsible for causing the event.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 (https://www.ietf.org/rfc/rfc2119.txt).

2 Objective and Scope

The objectives for this policy are:

- To assure there are system audit trails to account for, respond to, and minimize the effect of incidents that can impact the system
- To assure the handling of audit log information is in compliance with applicable laws and regulations

3 Roles and Responsibilities

3.1 System Administrator

The System Administrator (SA) is responsible for the collection of video footage, log files, and configuration files from the physical access control system, intrusion detection system, and network. These materials are collected during Key Ceremonies or during maintenance activities performed inside the Key Management Facility.

3.2 Ceremony Administrator

The Ceremony Administrator (CA) is responsible for the successful execution of the Key Ceremony in accordance with the script. The CA collects audit logs generated by the signing system during Key Ceremonies. It is the CA’s responsibility to confirm that all required materials are enclosed in the audit bundle.

3.3 Internal Witness

The Internal Witness (IW) provides an oversight role during the Key Ceremony and during audit materials collection. The IW's annotated script is the official log of the Key Ceremony's execution. Along with the CA, the IW helps ensure that the script is included in the audit bundle.

3.4 Policy Management Authority Chair

The Root Zone KSK Operator Policy Management Authority (PMA) Chair is responsible for generating and archiving audit trails related to the PMA meetings.

3.5 RZ KSK Operations Security

The RZ KSK Operations Security (RKOS) is responsible for monitoring, collecting, and archiving audit logs to ensure all audit logs are generated and kept as planned.

4 Security Requirements

4.1 Availability

The organization MUST be able to account for any event within a reasonable time and to be able to compile reports following each Key Ceremony.

4.2 Integrity

The organization MUST maintain the integrity of the audit information at all times.

5 Security Controls

This section defines the security controls required to mitigate identified vulnerabilities to an acceptable level of risk.

5.1 Security Management

The RZ KSK PMA MUST maintain and periodically review (at least annually) this policy, including the risk assessment.

Reviews MUST be documented in the change log of this document, and the following roles and responsibilities MUST be assigned:

5.1.1 RZ KSK PMA

The PMA is a committee responsible for overseeing the lifecycle of all policy documents relating to the RZ KSK Operations, including this policy. Refer to the PMA charter for a complete list of responsibilities and members.

5.1.2 RKOS

The RKOS function is a security support and coordination role responsible for:

- Following up on incident reporting
- Providing assistance to external auditors
- Conducting internal audits
- Initiating security awareness activities
- Providing security training
- Providing security expertise guidance to the PMA
- Overseeing the lifecycle management of the RZ KSK Operator function
- Ensuring all related documentation is maintained

Any changes or deviations from this policy MUST be approved by the PMA and documented to maintain an audit trail.

5.2 Types of Events Recorded

The following categories of security-related events MUST be recorded:

- Events specific to lifecycle management of the RZ KSK
- Events related to signing data
- Events related to physical access control
- Actions performed as part of the incident handling process
- Access to audit information
- Events related to system lifecycle management
- Evidence from a Key Ceremony
- Self-assessment and configuration reviews

Each event MUST be logged with the date and time, identification of the entity triggering the event (if applicable), and type of event.

5.3 Audit Log Collection

Automated audit data MUST be generated and recorded at the application and operating system level. Manually generated audit data MUST be recorded on paper by the responsible IW.

After each completed Key Ceremony, the CA MUST collect the electronic audit log information at the generating host and copy it onto at least two portable media devices. Paper-based documents MUST be copied and attested.

5.4 Audit Log Reviews

After each ceremony, audit logs MUST be reviewed for significant security and operational events by at least two individuals from different roles with the competence of recognizing anomalies and deviations from the Key Ceremony script. Evidence of such review MUST be provided.

Audit log reviews MUST include some form of verification that the log has not been tampered with along with an investigation of any alerts or irregularities in the logs. Actions performed based on audit log reviews MUST also be documented.

5.5 Audit Log Protection

Audit logs MUST be kept offline and protected with an audit log handling procedure that includes mechanisms to protect the information from unauthorized viewing, modification, deletion, and other tampering.

Everyone except authorized Trusted Persons MUST NOT be able to obtain direct access to the audit information. Access authorizations and the procedures for protecting the audit information MUST be specified in the “Audit Logging Procedure” document.

5.6 Audit Data Retention

All audit data collected MUST be retained onsite for at least one year after creation and MAY then be archived in an offsite storage facility. All audit data MUST be retained and remain accessible for at least 10 years.

The media holding the audit data and the applications required to process the information MUST be maintained to ensure that the archived data can be accessed for the entire duration of the retention period.

5.7 Audit Log Backups

All audit log information MUST be backed up to an offsite storage facility promptly after each key ceremony.

6 Documentation and Accountability

All RZ KSK Operator processes MUST be fully documented so as to accurately reflect current practices. For each of these processes, there MUST at all times be a designated employee formally charged not only with keeping this documentation up-to-date, but also with managing each process so it continues to serve all the purposes intended by management.

7 Log and Audit Trail Disclosure

System logs and application audit trails MUST NOT be disclosed to any person outside the team of individuals who ordinarily view such information in order to perform their jobs or investigate incidents. The RKOS MUST approve all exceptions in advance.

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
PMA	Root Zone KSK Operator Policy Management Authority
PTI	Public Technical Identifiers
RKOS	Root Zone 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 4: Simplified the security requirement language.
- Section 5.1: Restructured the RKOS responsibilities as a bulleted list.
- Sections 5.3, 5.4, 5.5, 5.6, and 5.7: Renamed the sections (except 5.7). Switched the order of the Audit Log Protection and Audit Data Retention sections. Merged the Audit Log Backups section into the Audit Data Retention section. Moved the Audit Log Collection section in front of the Audit Log Reviews section.
- Section 5.4: Clarified who can obtain direct access to audit information.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5: Audit Log Collection and Audit Log Protection existed twice: Removed duplicate subsections.
- Section 5.3: Removed the paragraph regarding the storage of information in an offsite storage facility since it is part of section 5.7 Audit Log Backups.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Overall: Uniformly specified “Practices Manager” as “PMA Chair”.
- Section 3.1: Specified “physical access control” as “physical access control system”.