Root Zone KSK Operator Incident Handling 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).

All personnel involving the Root Zone Key Signing Key (RZ KSK) have the duty to protect the confidential information against unauthorized usage, access, modification, destruction, disclosure, and transfer, whether accidental or intentional, and report security incidents, violations, and other problems to the RZ KSK Operations Security (RKOS) on a timely basis so prompt action may be taken.

Note that it is not the task of non-technical personnel to assess the severity or urgency of such problems. The person identified by the RKOS to immediately respond to all such reports will make this assessment.

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 handling security incidents or potential security incidents.

3 Roles and Responsibilities

All details pertaining to the security incidents are provided only to appropriate stakeholders such as RKOS, Physical Access Control Manager (PACM), and Root Zone KSK Operator Policy Management Authority (PMA). These stakeholders MAY share incident information with each other. These stakeholders SHALL NOT discuss security incident details openly or with inappropriate personnel.

3.1 RZ KSK Operator Policy Management Authority

The RZ KSK PMA is comprised of PTI and ICANN representatives from functional groups of both organizations. The PMA consists of two types of members: voting members and subject matter experts. All critical decisions related to RZ KSK operation are made by this group. The PMA is responsible for decisions to disclose these incident reports and for coordination with ICANN’s executive and communications teams.

3.2 RZ KSK Operations Security

RKOS is responsible for assessing the incident situation and providing advice to the PACM and PMA, acting as a facilitator and coordinator for all parties involved in handling the incident, and maintaining an audit trail throughout the process.

3.3 Physical Access Control Manager

The PACM approves physical access privileges to Key Management Facilities based on the information provided by the RKOS.

4 Incident Handling Procedures

4.1 Reporting

All security-related issues for RZ KSK operations MUST be reported to the RKOS. Send the information below immediately to cbo@iana.org or root-ksk-pma@iana.org and inform the personnel you have a potential security incident and would like to initiate the incident response process.

Type of Information	Contents
Title	Put "Urgent: Potential Security Incident Report" in the title and flag the email priority "Highest".
Date/Time/ Location	Describe the detection date and time with the location of the potential incident.
Contact Information	List the name, department, phone number, and email address of the personnel who detected the potential incident.
Incident Category	Refer to the Incident Category section (8) and specify which category the reporter thinks applies to the potential incident.
Incident Classification	Refer to the Incident Classification section (7) and specify which classification the reporter thinks applies to the potential incident.
Incident Description	Provide a brief description of the incident. Describe what happened, how it happened, the factors leading to the event, the substances or objects involved, etc.
Actions Taken	Describe the actions taken, if any.
Potential Loss	Describe what the potential loss is, if possible.
Witness	Provide contact information for any personnel other than the reporter who know about or witnessed the potential incident.

The incident classification examples below are a reference for personnel for incident reporting purposes. The actual incident rating will be performed by the RKOS.

Severity	Classification	Description	Initial Response
5	Extreme	Total loss of business, system, property, or trust; damage impossible to recover from	Within 1 hour
4	Major	Permanent partial loss of business, system, property, or trust; damage difficult to recover from	Within 4 hours
3	Moderate	Long-term loss of business, system, property, or trust; damage possible to recover from	Within 48 hours
2	Minor	Short-term loss of business, system, property, or trust; damage easy to recover from	Within 48 hours
1	Negligible	No loss of business, system, property, or trust; no damage	Within 1 business day

The incident category examples below are a reference for personnel for incident reporting purposes. The actual incident categorization will be performed by the RKOS.

Incident Category	Description
Denial of Service	Denial of service (DoS) or distributed DoS (DDoS) attacks that will affect the KSK operations.
Policy Violation	Any activity that would possibly violate the policies and procedures for RZ KSK operations, such as unauthorized escalation of privileges or a deliberate attempt to subvert access controls.
Compromised Information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or intellectual property.
Compromised Asset	A compromised host, network device, application, user account, etc. This includes malware-infected hosts where an attacker is actively controlling the host.
Compromised Facility	A physical break-in to a Key Management Facility.
Unlawful Activity	Theft, fraud, human safety, or computer-related incident of a criminal nature, likely involving law enforcement, global investigations, or loss prevention.
Hacking/Cracking	Reconnaissance or suspicious activity originating from inside the corporate network.
Email	Spoofed email and other email security-related events.
Multi-Factor Incident	An incident to which more than one incident category applies.
Equipment Failure	An incident in which equipment has a failure or malfunction.
Other	An incident that could not be classified with any of the above scenarios. Requires a detailed description of the incident.

4.2 Assessment

Once the potential incident is reported to the RKOS, the RKOS MUST conduct data collection and perform an initial incident assessment in order to determine the scope and impact to categorize the incident. Then the RKOS MAY establish a response team to remediate the situation.

4.3 Remediation

RKOS (with the assistance of the response team if required) MUST develop a proposed remediation plan. This plan MUST be approved by the PACM if the incident involves physical access control and other facility-related incidents, otherwise the approval of the plan MUST be escalated to the PMA.

The assessment and remediation effort MUST be repeated until the termination of the incident response is declared by the RKOS. Upon termination of the incident response process, RKOS MUST determine if any additional actions are necessary.

Appendix A: Acronyms

DDoS	Distributed Denial of Service
DoS	Denial of Service
ICANN	Internet Corporation for Assigned Names and Numbers
KSK	Key Signing Key
PACM	Physical Access Control Manager
PMA	Root Zone KSK Operator Policy Management Authority
PTI	Public Technical Identifiers
RFC	Request for Comments
RKOS	RZ KSK Operations Security
RZ	Root Zone

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 1.0 to 3.0 to match the version of other documents.
- Section 2: Added an Objective and Scope section.
- Section 3: Rewrote the introduction to the section. Added explanation of who stakeholders may share incident information with.
- Section 3.2: Clarified the responsibilities for the RZ KSK Operations Security role.
- Section 3.3: Added a definition of the Physical Access Control Manager role.
- Sections 4 through 8: Merged all the sections into a new Section 4. Made Reporting the new Section 4.1, and added the old Section 7 and Section 8 material to it. Made Assessment the new Section 4.2 and Remediation the new Section 4.3.
- Section 4.1: Clarified what the Incident Description should entail.
- Section 4.2: Added a caveat to the last sentence to indicate the action may not always be needed.
- Section 4.3: Clarified what RKOS must do after incident response process termination.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Section 4.1: Added two new incident categories: Equipment Failure and Other.
- Section 4.2: Updated Incident response procedure regarding response teams.
- Section 4.3: Clarified role responsibility.

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