# Root Zone KSK Operator Physical Security Policy

**Version 3.4**

Root Zone KSK Operator Policy Management Authority

19 October 2022

# 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 policy is to ensure that any risks associated with physical security are properly mitigated to an acceptable level, and that this level of risk is managed and maintained over time.

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 objectives of the physical security process are to:

- Deter, prevent, and detect any theft, tampering, or unauthorized use of the RZ KSK operational components, whether covert or overt (protect the integrity of the private key)
- Protect against physical damages to the RZ KSK operational systems, whether natural or man-made, and support the agreed service level in terms of availability of the system (protect system availability)

The critical system components protected by the physical security process are:

- The hardware components, specifically the Hardware Security Module (HSM) and the Personal Computer (PC)
- The activation material consisting of multiple sets of seven (7) Crypto Officer (CO) smartcards
- Encrypted backup of private key material stored on smartcards
- The audit information, which MAY consist of both hard copies and portable computer media
- Portable computer media used to store the signing software

This policy is applicable to all people involved in the RZ KSK Operator function.

The staff involved in the RZ KSK Operator function MUST comply with the policies found in this and other related information security documents. Staff who deliberately violate this or other information security policy statements will be subject to disciplinary action up to and including termination.

# 3 Roles and Responsibilities

The following roles and responsibilities MUST be assigned:

## 3.1 RZ KSK Operator Policy Management Authority

The Root Zone KSK Operator Policy Management Authority (PMA) is a committee responsible for overseeing the lifecycle of all policy documents relating to RZ KSK Operations, including this policy. Refer to the PMA charter for a complete list of responsibilities and members.

## 3.2 Physical Access Control Manager

The Physical Access Control Manager (PACM) as elected by the PMA is responsible for assigning physical access control credentials, maintaining the list of assigned authorizations and credentials, pre-authorizing entry into Key Management Facilities, and being the point of contact for the facility and alarm central provider for security-related matters.

## 3.3 RZ KSK Operations Security

The RZ KSK Operations Security (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
- Maintaining all related documentation

# 4 Security Requirements

## 4.1 Availability

The organization MUST be able to accommodate a Key Ceremony (with production key material) well within 30 days notice. (Note: Although availability is only required for Key Ceremonies, emergency repairs to the systems that maintain physical security, such as alarm systems, require 24x7 access.)

## 4.2 Integrity

The integrity of the RZ KSK private key component MUST to the utmost possible extent be maintained, whereas undetected theft, tampering, or unauthorized use of the private component of the RZ KSK is completely unacceptable.

# 5 Security Controls

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

## 5.1 Security Management

This policy MUST be maintained and periodically reviewed at least annually by the RZ KSK PMA. Reviews MUST be documented in the change log of this document.

## 5.2 Physical Access Control Management

The PACM MUST maintain a list of assigned access control authorizations for the Key Management Facility and assign and revoke access control credentials in accordance with this policy.

## 5.3 Perimeter Protection

The critical components of the signer systems (when not under constant observation of at least two Trusted Persons) MUST be protected by a minimum of four tiers of physical security, with access to lower tiers required before gaining access to higher tiers. Each tier is REQUIRED to provide reasonable resistance to forced entry and to be increasingly difficult to force through as one reaches higher tiers.

Sensitive Domain Name System Security Extensions (DNSSEC) operational activity and any activity related to the lifecycle of the RZ KSK occur within these restrictive physical tiers. Tiers MAY share a common barrier, if that barrier can be considered stronger than the tiers sharing it.

Doors, locks, and other access control mechanisms are considered part of their respective tier, and SHOULD NOT be significantly weaker than any other part of that tier.

## 5.4 Physical Access Control

All tiers MUST enforce individual access control for entry through the use of multifactor authentication, where one factor is REQUIRED to be based on tokens implementing strong cryptographic and tamper protection mechanisms.

In the event of a power failure, all doors controlled by the access control system MUST fail in a secure (locked) state.

Areas used for cryptographic operations MUST enforce dual access control and monitor dual occupancy. Unescorted personnel, including untrusted employees and visitors, MUST NOT be allowed into such secured areas. Anyone being escorted in or out of the facility MUST be manually logged with name and time of entry or exit.

The RZ KSK Operator's signer systems MUST be protected by a minimum of four tiers of physical security. Access to lower tiers is REQUIRED before gaining access to higher and more restrictive tiers. Access to tiers 3 through 6 MUST be controlled by the RZ KSK Operator's physical access control system.

Notice of entry MUST be given to the PACM via email or verbally prior to accessing any tiers of the Key Management Facilities (KMFs).

For physical access control, the following roles and their authorizations are defined:

### 5.4.1 Ceremony Administrator

Physical access restrictions for the Ceremony Administrator (CA) role:

- Unescorted access: MAY access Tier 3
- Escorted access by Internal Witness (IW): MAY access Tiers 4 and 5

### 5.4.2 System Administrator

Physical access restrictions for the System Administrator (SA) role:

- Unescorted access: MAY access Tier 3
- Escorted access by IW: MAY access Tier 4

### 5.4.3 Internal Witness

Physical access restrictions for the IW role:

- Unescorted access: MAY access Tier 3
- Escorted access by CA or SA: MAY access Tiers 4 and 5

### 5.4.4 Safe Security Controller

Physical access restrictions for the Safe Security Controller (SSC) role:

- Escort is REQUIRED at all times, especially when accessing Tier 6

## 5.5 Monitoring of Secure Areas

Physical access to each tier MUST be automatically logged by the access control system maintained by the RZ KSK Operator. The logs MUST periodically be transferred to both the RZ KSK Operator and the monitoring service provider in a timely manner.

Communication with the monitoring system MUST itself be monitored, and any failure to communicate with the monitoring system MUST be treated as an intrusion.

All tiers SHOULD be constantly video monitored and MUST be monitored for unauthorized access, power failures, smoke/fire, water, and extreme environmental fluctuations at all times. Any access not pre-authorized by the PACM MUST be treated as an intrusion.

Closed circuit television (CCTV) video recording of secure areas in between ceremonies is not considered part of the audit information. It SHOULD be archived for at least six (6) months. The facility provider MAY manage the CCTV.

## 5.6 Incident Response

The following events MUST initiate an incident response that is aligned with the Incident Handling Procedure document:

- Intrusion, tampering, or environmental event detection (alarm signal triggered): If the monitoring service provider receives an alarm signal, the monitoring service provider MUST contact the facility provider's onsite security staff to confirm any event and notify the RKOS or PACM. The onsite security staff MUST remove any person within the secured area or call law enforcement for assistance, and MUST provide reporting to the RKOS or PACM. The onsite staff MUST take appropriate measures to limit the effect of environmental events.
- Access without pre-authorization: If the monitoring service provider receives a notification of entry without prior notification of such an event by the PACM, that event MUST be treated as an intrusion.
- Warning signal: All warnings MUST be promptly investigated by RKOS and/or PACM, and an incident report MUST be generated when the triggering event is deemed to be substantial.

## 5.7 Power and Air Conditioning

The facility provider SHOULD provide heating, ventilation, and air conditioning equivalent to what would be required for an office space.

The facility provider SHOULD provide emergency power outlets to be used for critical components at Key Ceremonies. The access control and monitoring system controlled by the RZ KSK Operator MUST have separate battery-based backup for independent operation of at least 30 minutes.

The ceremony room SHOULD provide emergency lighting which automatically and instantly comes on in the event of a power failure to prevent blackout of the ceremony room and to facilitate an orderly system deactivation and evacuation.

All Key Management Facility access control systems and intrusion systems MUST be located such that they have ready access to two (2) electrical power substations.

## 5.8 Water Exposure

The containers (safes in combinations with any tamper-evident bags) used to store critical components MUST provide ingress protection from dripping water and spray commensurate to what might be caused by a sprinkler system.

To provide some protection from extensive flooding, the most critical components of the system (the HSMs) MUST be stored in the upper compartment of the safe.

## 5.9 Fire Detection and Suppression

The facility provider SHOULD provide automatic fire suppression and detection mechanisms that are automatically activated in the event of a fire.

Within the ceremony room, there SHOULD be fire extinguishing devices based on both carbon dioxide and dry powder available for manual suppression of small fires, and these devices MUST be maintained.

Fire prevention and protection measures MUST comply with local fire safety regulations.

## 5.10 Protection from Electromagnetic Radiation

Areas used for cryptographic operations and storage of critical components MUST be located at least 10 meters (30 feet) from any outside unmonitored, unrestricted, and publicly accessible area.

## 5.11 Disaster Recovery Site

The RZ KSK Operator MUST maintain disaster recovery capabilities for its DNSSEC operations by (under normal circumstances) maintaining more than one Key Management Facility which implements the requirements of this physical security policy.

All Key Management Facilities MUST at any point in time hold the data required for production, and MUST be evenly utilized to ensure capabilities are maintained at all sites.

## 5.12 Media Storage

Any media or device containing production private key material MUST NOT be handled, stored, or transported outside the Key Management Facilities at any time in any form. Newly generated private keys MUST NOT be taken into production until distributed and safely stored at all Key Management Facilities.

All other media containing production software and data, audit, archive, or backup information MUST be stored within the facilities or at an offsite storage facility.

Any media, when not under the constant observation of a Trusted Person, MUST be stored within signed and sealed, serial-numbered, tamper-evident bags.

## 5.13 Offsite Storage Facility

For each Key Management Facility, there MUST be an offsite storage facility supplying a compartment for storage of production software and data, audit, archive, or backup information. The offsite storage facility MUST be located at least five (5) kilometers away from the Key Management Facility. Access control, fire and flood protection, and environmental control MUST at least be commensurate to that of a bank safety deposit box.

The facility MUST be given a list of persons who may access the storage facility, and this list MUST be maintained. The point of contact for the facility MUST be the CA or the RKOS.

Access to the offsite storage facility MUST be limited to the CA or the RKOS.

## 5.14 Media Disposal

Sensitive documents and materials MUST be shredded before disposal. Media used to collect or transmit sensitive information MUST be rendered unreadable before disposal.

Cryptographic devices MUST be physically destroyed or zeroized in accordance with the manufacturer's guidance prior to disposal. Other waste MUST be disposed of in accordance with normal waste disposal requirements.

The RZ KSK Operator MUST verify the data-specific methods of all third parties contracted for destruction of equipment containing sensitive data.

RKOS MUST maintain an inventory of production equipment and equipment that has been taken out of commission. This inventory MUST also reflect all actions taken to destroy or zeroize stored information.

# 6 Equipment Maintenance

All information systems equipment used for production processing MUST be maintained in accordance with the supplier's recommended service intervals and specifications, with all repairs and servicing performed only by qualified and authorized maintenance personnel. Preventive maintenance MUST be regularly performed on all computer and communications systems.

# 7 Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises SHOULD be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

# 8 Communications Equipment Areas

Telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing communications equipment MUST be kept locked at all times and MUST NOT be accessed by visitors without an authorized technical staff escort to monitor all work being performed.

# 9 Key Management Facility Tours

Public tours of the KMFs MUST NOT be conducted unless an exception is made by the PACM.

# 10 Physical Entry Controls

Secure areas SHOULD be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Access to key management facilities MUST be physically restricted to limit access to those with a need to know.

## 10.1 Identification Badges

When in Key Management Facilities, all unescorted persons MUST wear an identification badge on their outer garments so they are clearly visible to all people with whom the wearer converses.

Any person who has forgotten their identification badge MUST obtain a one-day temporary badge by providing a driver's license or another piece of picture identification.

## 10.2 Badge-Controlled Access

Each person MUST present his or her badge to the badge reader before entering every controlled door within the RZ KSK Operator's premises.

Authorized persons MUST NOT permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances.

## 10.3 Unauthorized Physical Access Attempts

People MUST NOT attempt to enter restricted areas in the RZ KSK Operator buildings for which they have not received access authorization.

## 10.4 Access Control System Records

The RKOS MUST maintain records of the persons currently and previously inside the RZ KSK Operator buildings and MUST securely retain this information for at least one year.

## 10.5 Bag Inspection and Prohibited Items

All briefcases, suitcases, handbags, and other luggage MUST be checked at reception if possible prior to entering the RZ KSK Operator Key Management Facility. RKOS SHALL inform attendees of the prohibited item policy prior to attendees entering Tier 3 of the Key Management Facility, and SHALL take reasonable steps to ensure compliance. Exceptions MAY be granted by RKOS when appropriate on a case by case basis.

## 10.6 Visitor Identification

All visitors MUST show government-issued picture identification and sign in prior to gaining access to restricted areas. Visitors are also REQUIRED to sign out when leaving.

## 10.7 Individuals Without Identification Badges

Individuals without a proper identification badge in a clearly visible place MUST be immediately questioned about their badge and if they cannot promptly produce a valid badge, they MUST be escorted to a reception desk, a guard station, or the person they came to see.

## 10.8 Unescorted Visitors

Whenever a staff notices an unescorted visitor inside a Key Management Facility, the visitor MUST be questioned about the purpose for being in a restricted area, and then be accompanied to a reception desk, a guard station, or the person they came to see.

# Appendix: Acronyms

| | |
|---|---|
| CA | Ceremony Administrator |
| CCTV | Closed Circuit Television |
| CO | Crypto Officer |
| DNSSEC | Domain Name System Security Extensions |
| HSM | Hardware Security Module |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IW | Internal Witness |
| KMF | Key Management Facility |
| KSK | Key Signing Key |
| PACM | Root Zone KSK Operator Physical Access Control Manager |
| PC | Personal Computer |
| 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 |
| SSC | Safe Security Controller |

# 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 5.1 and 5.5: Moved text about Roles and Responsibilities were moved to Section 3.

**Revision 3.1 - 28 October 2019**

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5.9: Removed independent fire monitoring. Provided by facility.
- Section 9: Approval will be provided by PACM.
- Section 10.4: Records will be maintained by RKOS.

**Revision 3.2 - 04 November 2020**

- Annual review: Update version information and dates.
- Section 5.6: Clarified warning signal detection incident response procedure.
- Section 10.5: Updated bag inspection procedure to consider facility provisions, and added a prohibited item handling to the procedure.

**Revision 3.3 - 22 September 2021**

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