Root Zone KSK Operator Personnel Security Policy

Version 3.5

Root Zone KSK Operator Policy Management Authority

12 October 2023

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).

Personnel security plays a critical role in the RZ KSK Operator function. Especially for key management, the majority of operations are performed manually. Personnel security MUST be strictly enforced in order to prevent devastating consequences that can potentially damage the RZ KSK Operator's reputation, and the perceived security of the Domain Name System Security Extensions (DNSSEC). Security concepts such as two-person integrity, dual control, and dual occupancy rely on successful personnel security enforcement. Negligence of personnel security will jeopardize multi-person control, which is one of the core concepts in key management.

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 this policy are to ensure that staff, contractors, and third-party users understand their responsibilities and are suitable for the roles in which they are considered. In addition, the policy seeks to mitigate the risk from internal threats such as sabotage, espionage, denial of service, and in extreme cases, terrorism.

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 information security 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

3.1 Human Resources Department

Executing background checks of personnel, retaining the resultant records, and conducting other sensitive investigations on staff whenever required are services provided to the RZ KSK Operator by ICANN's Human Resources (HR) department.

3.2 RZ KSK Operations Security

RZ KSK Operations Security (RKOS) monitors personnel security activities and provides periodic reports to the Physical Access Control Manager (PACM). RKOS is also responsible for enforcing this policy.

3.3 Physical Access Control Manager

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

The PACM reviews the list of key management role assignments for Ceremony Administrators, Internal Witnesses, System Administrators, and Safe Security Controllers annually.

4 Trusted Roles

Individuals who have access to or control over operations of the RZ KSK are called “Trusted Persons” and perform “Trusted Roles” as described below. Persons seeking to become or remain a Trusted Person for RZ KSK operations MUST successfully complete the screening requirements set out in the DNSSEC Practice Statement (DPS).

Trusted Persons include all staff, contractors, and consultants who have access to or control operations that may materially affect:

- Generation and protection of the private component of the RZ KSK
- Secure export or import of any public components
- Zone file data

Trusted Roles include, but are not limited to:

- System Administrators
- Crypto Officers
- Recovery Key Share Holders
- Safe Security Controllers
- Internal Witnesses
- Ceremony Administrators
- RZ KSK Operations Security

5 Background Check

The RZ KSK Operator REQUIRES personnel seeking to become or remain a Trusted Person to submit to a background check. To the extent permitted by the national laws of the Trusted Person or candidate’s country of residence, background checks MUST include the following and MUST be repeated at least every five (5) years:

- Criminal history (felony, misdemeanor, and government watch lists)
- Professional references
- Credit/financial records

In the absence of exceptional circumstances, candidates or existing Trusted Persons with convictions or decisions as listed in (A) to (J) below MUST be considered for rejection for Trusted Roles, including removal from the program for existing Trusted Persons.

A. Within the past five (5) years, has a pattern of adverse accounts or negative items in the financial history. The presence of one or more factors on the following non-exhaustive list MAY weigh toward showing a pattern of precarious financial history indicating a lack of financial responsibility: (i) the candidate has filed bankruptcy, (ii) the candidate has incurred a pattern of late payments to a significant number of creditors, and (iii) the candidate has significant number of accounts referred to debt collection agencies.
B. Within the past five (5) years, has been convicted of any crime related to financial or corporate governance activities, has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that the RZ KSK Operator deems as the substantive equivalent of any of these
C. Within the past five (5) years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of funds of other parties
D. Within the past five (5) years has been convicted of any willful tax-related fraud or willful evasion of tax liabilities
E. Within the past five (5) years has been convicted of perjury, forswearing, failing to cooperate with a law enforcement investigation, or making false statements to a law enforcement agency or representative
F. Has ever been convicted of any crime involving the use of computers, telephony systems, telecommunications, or the Internet to facilitate the commission of crimes
G. Has ever been convicted of any crime involving the use of a weapon, force, or the threat of force
H. Has ever been convicted of the illegal sale, manufacture, or distribution of pharmaceutical drugs, or been convicted or successfully extradited for any offense described in Article 3 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988
I. Has ever been convicted or successfully extradited for any offense described in the United Nations Convention against Transnational Organized Crime (all Protocols),
J. Fails to provide a good faith effort to disclose all relevant information relating to the aforementioned items (A) to (I).

Due to differences in national laws and other difficulties that may limit the RZ KSK Operator's ability to conduct checks on all of the above, if a background check is found lacking, the RZ KSK Operator MAY request the personnel being selected for a Trusted Role to submit professional references. This is in

addition to the signed self-declaration, shown in appendix B, that all personnel applying for a Trusted Role must submit.

5.1 Background Check Procedure

The HR Department, with its selected vendor, is responsible for executing the background checks for all existing and candidate Trusted Persons.

1. RKOS MUST provide a list of existing and candidate trusted persons to HR for background check.
2. RKOS MUST provide all Trusted Persons and candidates with the name of the vendor that will perform the background check.
3. The vendor MUST provide the background check authorization form to all Trusted Persons and candidates. These individuals MUST complete the authorization form. A copy of the collected information MAY be obtained if the option to receive a copy is selected.
4. The vendor MUST conduct a background check and forward the collected information to HR for review.
5. HR MUST evaluate the collected information if convictions or decisions are present as listed in (A) to (J). If decisions or convictions are found, HR MUST discuss all relevant information relating to the potential negative result with the individual.
6. HR MUST notify RKOS and Legal staff relevant to managing the assignment of Trusted Persons with the results of the background check to determine the appropriate course of action. Details of the results MUST be kept confidential unless the information is deemed to be public knowledge.
7. HR MUST securely retain all background check results for up to five (5) years. Disposal of the results and all relevant information pertaining to the background check MUST be performed in a manner so it cannot be read or reconstructed.

6 Non-Disclosure Agreements

All staff, contractors, and consultants MUST personally sign a non-disclosure agreement. The provision of a signature MUST take place before work begins, or if a worker has been working without a non-disclosure agreement, a signature MUST be provided as a condition of continued employment.

7 Training Requirements

The RZ KSK Operator MUST provide its personnel with training when hired, as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. The RZ KSK Operator MUST periodically review and enhance its training programs as necessary.

The RZ KSK Operator's training programs MUST be tailored to the individuals' responsibilities and MUST include the following as relevant:

- Basic Domain Name System (DNS) and DNSSEC concepts
- Job responsibilities
- Use and operation of deployed hardware and software
- Security and operational policies and procedures
- Incident and compromise reporting and handling
- Disaster recovery and business continuity procedures

The RZ KSK Operator MUST provide refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

8 Sanctions for Unauthorized Actions

Appropriate disciplinary actions will be taken for unauthorized actions with respect to this document and/or other violations of the RZ KSK Operator's security policies and procedures. Disciplinary actions MAY include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

9 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants MAY be used to fill Trusted Roles. Any such contractor or consultant MUST be held to the same functional and security criteria that apply to any staff of the RZ KSK Operator in a comparable role. Independent contractors and consultants who have not completed or passed the background check process MAY be permitted access to the RZ KSK Operator's secure facilities only to the extent that they are escorted and directly supervised by Trusted Persons at all times.

Temporaries, consultants, contractors, and outsourcing organization staff MUST NOT be given access to sensitive information or be allowed to access critical information systems unless they have gone through a background check commensurate with the background checks given to regular staff.

10 Documentation Supplied to Personnel

The RZ KSK Operator MUST provide its staff the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

11 Termination of Employment

11.1 Staff Termination Responsibility

In the event that an employee, consultant, or contractor is terminating his/her relationship with PTI or ICANN, the worker's immediate manager MUST ensure that all property in the custody of the worker is returned before the worker leaves PTI or ICANN, notify all administrators handling the access credentials, physical keys, and other assets used by the worker as soon as the termination is known, and terminate all other work-related privileges of the individual at the time the termination takes place.

11.2 Notification of Worker Terminations

All staff MUST be immediately notified as soon as a worker has been terminated. With each such notice, the HR Department MUST regularly remind staff that departed workers are no longer permitted to be on the RZ KSK Operator's property (unless escorted by an employee), use PTI or ICANN resources, or in any other way be affiliated with PTI or ICANN.

11.3 Involuntary Terminations

In all cases where information technology support workers are involuntarily terminated, they MUST be relieved of all of their duties immediately, REQUIRED to return all PTI or ICANN equipment and information, and escorted while they pack their belongings and walk out of the RZ KSK Operator's facilities. This type of termination MUST take place with a presence of a security personnel.

11.4 Escorting Involuntarily Terminated Workers

In every case where workers are involuntarily terminated by PTI or ICANN, the termination MUST take place in the presence of a security guard. These workers MUST immediately pack their personal belongings in the presence of the guard and be shown to the door. These workers MUST also be informed that they MUST NOT reenter the building unless invited to do so by management.

11.5 Return of Assets and Removal of Access Rights

All staff, contractors, and third-party users MUST return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.

At the time that any employee, consultant, or contractor terminates his or her relationship with PTI or ICANN, all PTI or ICANN property including, but not limited to, building keys, proximity badges, smartcards, and other access credentials MUST be returned. These terminating individuals MUST inform management about all PTI or ICANN property they possess, as well as all computer system privileges, building access privileges, and other privileges they have been granted.

In addition to collecting the access credentials, all access rights MUST be terminated on the access control system as soon as possible. If applicable, any type of lock combination and keys (if applicable) MUST be changed.

Appendix A: Acronyms

DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPS	DNSSEC Practice Statement
HR	Human Resources
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: Self Declaration

Trusted Community Representative Declaration

I understand that I will hold a trusted role in the Root Zone DNSSEC Key Signing Key operations, undertaken as a joint effort by the Root Zone Management Partners: Internet Corporation for Assigned Names and Numbers (ICANN), Public Technical Identifiers (PTI), and Verisign.

Aside from background checks that were performed as part of the requirement from the DNSSEC Practice Statement (DPS) and the "trust" notion in becoming a Trusted Community Representative, I, _____ uphold the highest honesty and integrity and hereby declare the following:

1. Within the past fifteen years, I have not been investigated for or convicted of a crime in any jurisdiction around the world related to fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

2. Within the past fifteen years, I have not been judged by any court or been the subject of any judicial determination, or in any type of dispute resolution proceeding, to have committed fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

3. Within the past fifteen years, I have not been disciplined by any government for conduct involving dishonesty, including, fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

4. I am currently not involved in any governmental, judicial, or regulatory proceeding or investigation that could result in a conviction, judgment, determination, or discipline of the type specified in 1, 2, or 3 above.

By signing this declaration, the undersigned attests that the aforementioned statements are true and accurate.

Date: _____

Signature: _____

Print name: _____

Appendix C: 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.
- Clarified which requirements apply to staff only and which apply to all users (employees, contractors, third parties, etc.)
- Sections 11.3 and 11.4 were combined.

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.
- Section 4: Updated list of roles

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Section 3.3: Consolidated duties from former section 3.4 previously assigned to PMA.
- Section 3.4: Duties reassigned to PACM in section 3.3, then removed.

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.
- Made minor editorial, formatting, and style changes.

Revision 3.5 - 12 October 2023

- Annual review: Update version information and dates.