Root Zone KSK Operator Password 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).

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

This document sets the minimum policy requirements for managing passwords and personal identification numbers (PINs) in the Root Zone KSK operation. This password policy covers the devices, systems, and services used in the Key Management Facilities (KMFs) that include, but are not limited to, the physical access control system, physical intrusion system, network firewalls, and streaming laptops. Systems and services that are provided to the RZ KSK Operator by ICANN are covered by ICANN's corporate password policy, which covers devices like corporate laptops, corporate email accounts, and access to corporate networks.

3 Roles and Responsibilities

3.1 User

Users are those who hold accounts with passwords or PINs that are used to access information assets related to the RZ KSK Operator function.

3.2 System Administrator

The SA is responsible for provisioning and terminating accounts, resetting passwords, and performing any other operations required for password management.

3.3 RZ KSK Operations Security

RZ KSK Operations Security (RKOS) is responsible for conducting periodic account reviews to ensure only authorized personnel have access to the systems.

4 User Password Management

4.1 Initial Password

Default passwords issued by an SA MUST be expired whenever possible, forcing the user to choose another password before the next logon process is completed. The initial password for a new user who is not onsite MUST be sent through a secure communications channel including, but not limited to, S/MIME or PGP encrypted email.

4.2 Password Change

Passwords MUST be changed within a reasonable timeframe when one of the authorized users of a shared account has been removed from the role.

4.3 Password Reset

Only the user who owns the account MAY request password changes and resets. A user MUST NOT, under any circumstances, delegate or otherwise request that another person handle this task on the user's behalf. RZ KSK Operator systems do not enforce limited attempts for password entry due to the low frequency of use, and physical compensating controls are in place to prevent unauthorized access attempts.

4.4 Password Change After Compromise

After either a suspected or demonstrated intrusion to a computer system, the attending SA MUST immediately notify the system’s users that an intrusion is believed to have taken place. The status of all passwords on that system MUST immediately be changed to expired, so these passwords will be changed at the time that the involved users next login. If a privileged user ID has been compromised by an intruder or another type of unauthorized user, all passwords on that system MUST be immediately changed.

4.5 Password Disclosure

A user MUST be authenticated in person to obtain a new or changed password. SAs MUST disclose passwords to a user providing two pieces of definitive evidence substantiating their identity if a new user ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of their account.

5 User Access Privilege Review

RKOS and SA MUST review the granted access and system privileges of users after each Key Ceremony. This review MUST determine whether the users have only those privileges necessary to perform their jobs and no additional privileges.

6 User Responsibilities

6.1 Password Structure

Users MUST NOT employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, a single word in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of normal speech. Users MUST NOT construct cyclical fixed passwords that combine a set of characters that do not change with a set of characters that predictably change.

Each password MUST be at least sixteen (16) ASCII characters long.
Each PIN must be at least six (6) digits long.

Passwords do not expire due to the extremely low frequency of use and other compensating controls that physically protect access to the devices that require passwords.

6.2 Storage of Passwords in Readable Form

Fixed passwords MUST NOT be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, computers without enforced access control mechanisms, plain text documents, or other locations where unauthorized persons might discover or use them.

6.3 Passwords on Different Systems

Users MUST employ different passwords on each of the systems to which they have been granted access. Users MUST NOT use the same password on multiple systems unless they have been informed by the RKOS that doing so will not unduly compromise security.

6.4 Public Password Disclosure

Passwords MUST NOT be written down and left in a place where unauthorized persons might discover them. Users MUST NOT write down or otherwise record a readable password and store it near the access device to which it pertains. Users MUST NOT write their passwords down unless they have effectively concealed such passwords in seemingly unrelated characters or they have used a coding system to conceal the password. Each user MUST immediately change his or her password if the password is suspected of being disclosed, or is known to have been disclosed to an unauthorized party.

6.5 Password Sharing

Passwords MUST NOT be shared or revealed to anyone other than the authorized user. An exception is made when first establishing a password or resetting a password. Computer accounts, user IDs, network passwords, and other access codes MUST NOT be used by anyone other than the person to whom they were originally issued.

Users MUST NOT provide their user IDs and/or passwords to data aggregators, data summarization/formatting services, or any other third parties. Such disclosures not only cause the involved users to be responsible for all damage a third party may cause, but this behavior is also justifiable cause to terminate the user's privileges.

Any user who is shown to have disclosed his or her password to anybody or to any organization, for whatever purpose, will have their system privileges immediately revoked.

6.6 Personal User IDs

Users MUST be responsible for all activity performed with their personal user IDs. They MUST NOT permit others to perform any activity with their user IDs, and they MUST NOT perform any activity with IDs belonging to other users.

6.7 Exploiting Systems Security Vulnerabilities

Users MUST NOT test or attempt to compromise internal controls unless this activity is specifically approved in advance in writing by RKOS. Users MUST NOT exploit vulnerabilities or deficiencies in information system security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted.

6.8 Handling of Cleartext Credentials

Users MUST NOT store cleartext authentication credentials anywhere, and MUST NOT set up or employ script files that contain a stored version of a PIN, a password, or a user ID which can be used to gain access to the information system. Likewise, these security parameters MUST NOT be stored anywhere on these devices unless they are in encrypted form.

Appendix A: Acronyms

ICANN	Internet Corporation for Assigned Names and Numbers
KSK	Key Signing Key
PIN	Personal Identification Number
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.
- Clarified which requirements apply to staff only and which apply to all users (employees, contractors, third parties, etc.)
- Section 3.1: Clarified the user’s responsibilities.
- Section 3.3: Clarified the responsibilities of RKOS.
- Section 4.1: Clarified that phones are not a secure communications channel.
- Section 6.8: Renamed the section and clarified the requirements for cleartext credentials.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 4.1: Removed reference to decommissioned systems.
- Section 6.1: Updated to reflect current password policy.
- Section 6.2: Updated to include plain text documents.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Section 2: Removed specific KMF locations which were not relevant.
- Section 5: Clarified user access review procedure.

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.

Revision 3.5 - 12 October 2023

- Annual review: Update version information and dates.
- Section 6.1: Password requirements updated to reflect recommendations made in NIST SP800-63B