Root Zone KSK Operator Physical Access Control Procedure

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 Root Zone Key Signing Key (RZ KSK) Operations MUST be conducted within physically protected environments that prevent damage to critical components and deter, prevent, and detect any unauthorized use of or access to critical components, whether covert or overt.

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 of this document is to define requirements and recommendations for physical access control procedures to be performed by designated personnel, systems, and other mechanisms.

3 Roles and Responsibilities

Those in the Physical Access Control Manager (PACM) role SHALL comprise the President of PTI or the President of PTI's delegate, along with other individuals appointed by the RZ Operator KSK Policy Management Authority (PMA). The PACM is responsible for assigning physical access control credentials, maintaining the list of assigned authorizations and credentials, pre authorizing entry into security facilities, and being the point of contact for the facility provider and alarm central provider for security-related matters.

4 Requesting Assignments of User Credentials

Figure 1 depicts the workflow for the PACM, RZ KSK Operations Security (RKOS), and the System Administrator (SA) for requesting assignments of user credentials.

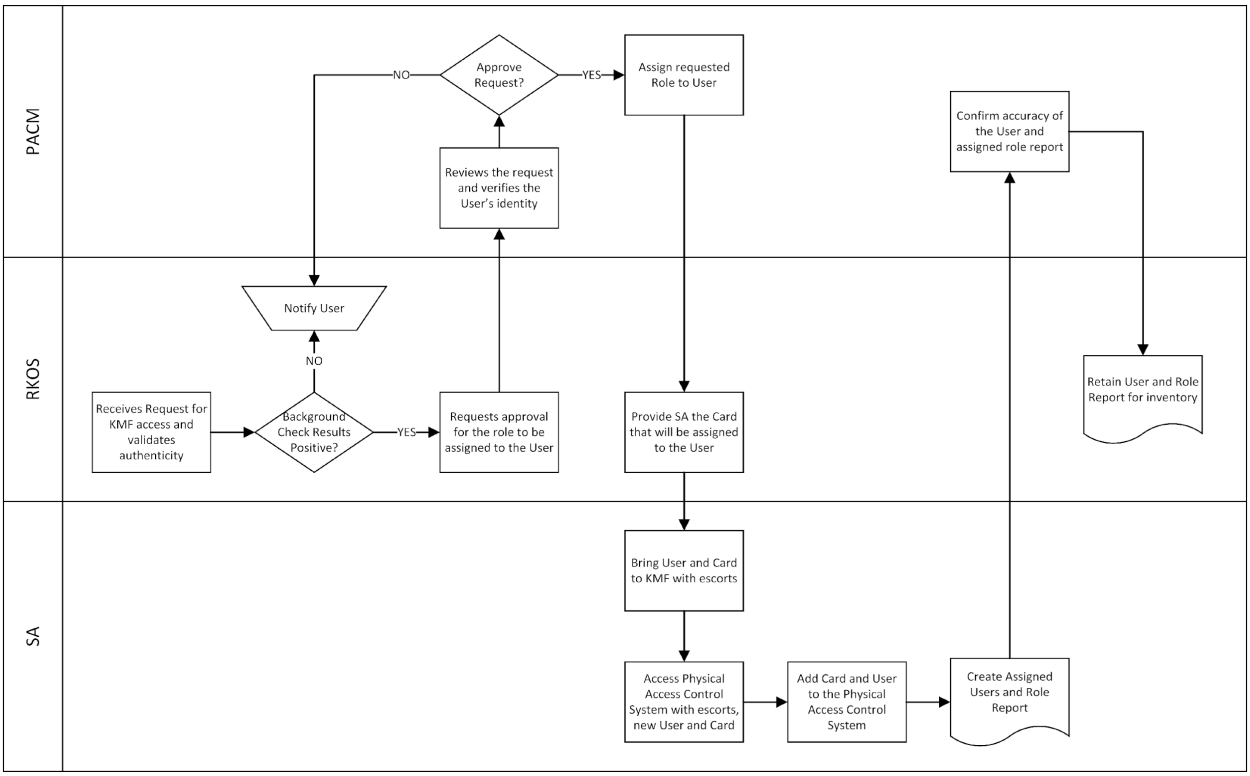

Figure 1: Workflow for requesting assignments of user credentials

4.1 PACM Authorization

1. RKOS receives the request for a new user. The descriptions of user roles are defined in section 5.4 of the Physical Security Policy document.
    a. RKOS MUST validate that background check results are positive through ICANN's Human Resources department before proceeding, then provide the PACM with the new user's information for review and approval.
    b. On a Secure Facility Role Authorization (manual or electronic), RKOS MUST document the role and user, and select an access card for the user. The RKOS MUST document the access card serial number that will be assigned to the user and retain a current list of authorized users and their card numbers. This list MUST be submitted to the PACM for review and approval of changes.
2. The PACM MUST communicate (email or voice) if the access request has been approved. The RKOS initiates the work with the SA.
3. After checking a government-issued photo ID, the RKOS provides an access card to the SA. This card MUST NOT be activated until the SA configures it within the physical access control system. The RKOS MUST secure an inventory of unprovisioned contactless access cards used for the physical access control system. The cards MUST be unusable until they have been personalized and assigned to a specific role using the physical access control system.

4.2 Physical Access Control System Configuration

1. The PACM grants access to the facility by notifying the monitoring provider of the planned entry. The Ceremony Administrator (CA) and Internal Witness (IW) MUST escort the new user (with access card) and the SA into Tier 5 to access the physical access control system. Note: CA and IW maintain escort roles only and MUST NOT hold codes for programming of new identities. SA is solely responsible for programming the access system.
2. The SA MUST enter the system PIN to configure room user access.
3. The SA MUST create the user account based on the authorized role and badge serial number.
4. The SA MUST print out a report containing the list of user accounts with assigned authorizations for review by the PACM.
5. The PACM MUST retain the user account and roles report for review.

5 Assigned User and Authorization Review

Reviewing assigned users and authorizations is performed annually and after each KSK ceremony. Figure 2 depicts the workflow for the PACM, RKOS, and SA for reviewing assigned users and authorizations.

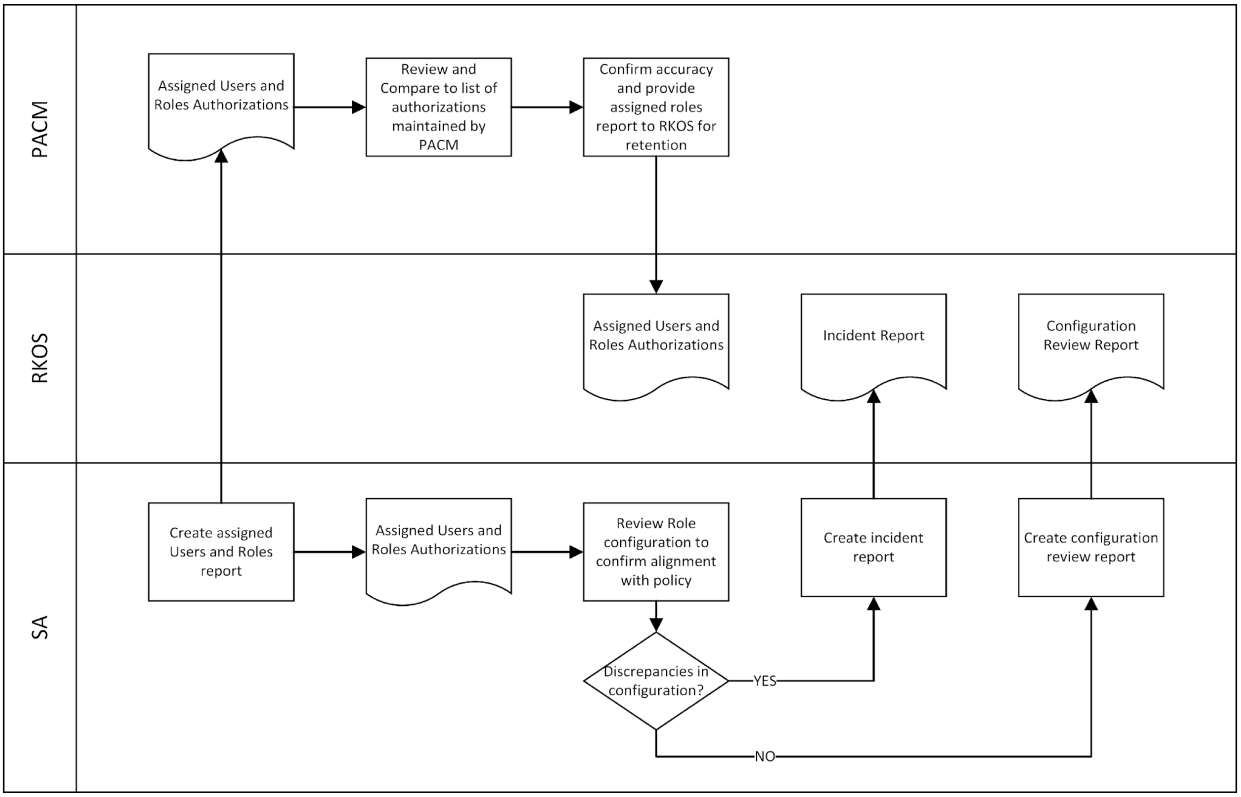

Figure 2: Workflow for reviewing assigned users and authorizations

1. To verify assigned users and role authorizations against the policy:

a. An authorized SA MUST generate a list of users with assigned roles, then confirm they are aligned with the policy.
b. SA MUST create an incident report if any discrepancies are found. Otherwise, a configuration review report MUST be generated and submitted to the RKOS.

2. To verify assigned users and role authorizations using the list of authorizations maintained by the PACM:
   a. An authorized SA MUST generate a list of users and their assigned roles, then submit it to the PACM for review.
   b. The PACM receives the report and MUST compare it with the maintained list of authorized users.

6 Revoking Access

Figure 3 depicts the workflow for the PACM, RKOS, and SA for revoking access.

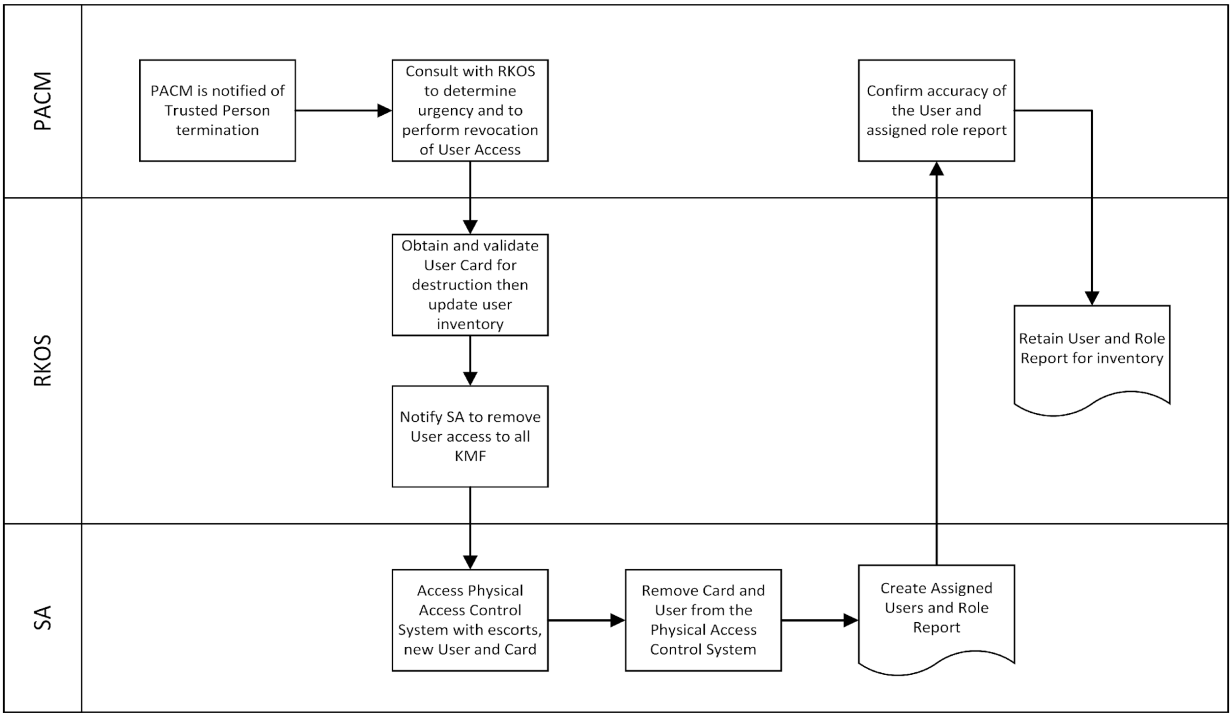

Figure 3: Workflow for revoking access

1. PACM is notified of the person holding a Trusted Role (email or voice). Then the PACM MUST notify the RKOS to obtain the terminated user's access card and to work with the SA to remove access at the next opportunity when CA, IW, and SA are present at the facility for other reasons.
2. With the authorization of the PACM, RKOS MUST destroy the access card.
3. If an access card is lost, it MUST immediately be reported to the RKOS as an incident. The RKOS MUST investigate the loss and provide a recommendation to the PACM on the urgency of revoking the card's access rights. The PACM MUST decide on how/when to revoke.
4. When removing access, the SA, escorted by the CA and an IW, MUST enter the facility and access the physical access control system. The SA MUST remove access from the system, generate a new Current User Report, and send it to the PACM to confirm access was removed.

5. The PACM receives the report and MUST confirm the accuracy of the list of users and their assigned roles. Then the PACM MUST report to the RKOS the result of the revision for retention.

7 Using Emergency Access

For emergency purposes (e.g., personnel safety, physical access control system failure), the facility MUST be equipped with keyed physical locks on all doors. Use of these keys MUST always trigger an alarm.

1. One physical key MUST be held by the facility provider.
2. The second key MUST be within a signed, sealed, tamper-evident bag placed in a bank box near each Key Management Facility.
3. Only the RKOS, as well as one trusted alternate (as designated by the PACM), MUST have access to the bank box.

8 Provisioning Access to the Key Management Facility

As the RZ KSK Operator's Root Domain Name System Security Extensions (DNSSEC) Key Management Facility (KMF) resides in a building managed by a third-party vendor, access to the building MUST be provisioned separately from the access to the room. Whoever is granted permanent access privileges to the KMF is eligible for access to the facility. The facility access MUST be provisioned under the supervision of the PACM or the RKOS.

Appendix A: Acronyms

CA	Ceremony Administrator
DNSSEC	Domain Name System Security Extensions
ICANN	Internet Corporation for Assigned Names and Numbers
IW	Internal Witness
KMF	Key Management Facility
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
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 1: Added an introductory paragraph.
- Section 2: Added an Objective and Scope section.
- Section 4: Added a brief explanation of Figure 1 and a caption for the figure.
- Section 5: Added a brief explanation of Figure 2 and a caption for the figure.
- Section 6: Added a brief explanation of Figure 3 and a caption for the figure.

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 6 Step 3: Specified "card" as "access card".

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.