Root Zone KSK Operator Emergency KSK Rollover Plan

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 with the Internet Corporation for Assigned Names and Numbers (ICANN).

This document defines the plan for handling emergency RZ KSK rollovers relating to KSK operations. An emergency KSK rollover would be initiated if the RZ KSK Private Key has been irrecoverably lost or compromised.

Loss or compromise could consist of the theft, loss, disclosure, unauthorized use, or reduction in the trustworthiness of the security of the KSK Private Key and its operation.

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 emergency rollover plan will be used only when the RZ KSK is lost or compromised. Only these two high-level scenarios are covered under this plan. Other incidents under which the RZ KSK is still operational and under which key signing operations can be resumed without significant interruption to service are addressed by the “Incident Handling Procedure” and the “Disaster Recovery and Business Contingency Procedure”.

2.1 Scenarios Covered Under this Plan

The following scenarios are covered within the scope of this plan:

2.1.1 KSK Compromise

Unable to secure the private key of the KSK due to:

- Broken algorithm
- Theft of KSK equipment in Key Management Facility (KMF)

2.1.2 KSK Loss

Unable to access the private key of the KSK due to:

- All Hardware Security Modules (HSMs) experience catastrophic failure
- All KSK backups are not functioning
- Theft of KSK equipment in KMF

3 Roles and Responsibilities

3.1 RZ Key Signing Key Operator

PTI performs the Root Zone Key Signing Key (RZ KSK) Operator function of generating the RZ KSK and signing the Root Keyset, including the Root Zone Zone Signing Key (RZ ZSK), using the KSK. The RZ KSK Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the KSK (the Trust Anchor) to the relying parties.

3.2 RZ Zone Signing Key Operator

The RZ ZSK Operator is Verisign performing the function of generating the RZ ZSK and signing the Root Zone File using the ZSK. The RZ ZSK Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the ZSK to the RZ KSK Operator for signing.

The RZ Zone Signing Key Operator serves in an advisory role to the parties involved in an emergency KSK rollover.

3.3 Root Server Operators

The Root Server Operators consist of 12 different professional engineering entities responsible for providing the root zone to the public via the 13 Root Zone Authoritative Name Servers.

3.4 Relying Party

A Relying Party is the entity that relies on DNSSEC, such as security-aware validating resolvers and other applications that perform validation of DNSSEC signatures.

3.5 RZ KSK Operator Policy Management Authority

The RZ KSK Operator Policy Management Authority (PMA) is comprised of representatives of PTI and ICANN. The PMA consists of two types of members: voting members and subject matter experts. All critical decisions related to the RZ KSK operation are approved by this group.

3.6 Physical Access Control Manager

The Physical Access Control Manager (PACM) approves physical access privileges to Key Management Facilities based on the information provided by the RKOS.

3.7 RZ KSK Operations Security

RZ KSK Operations Security (RKOS) is responsible for assessing emergency situations and providing advice to the PMA, while ensuring the integrity, accountability, and audit trail of the entire rollover process.

4 Incident Management

If the RZ KSK Operator detects an event that has led to or could have led to a compromise of any of the security mechanisms, an investigation will be performed in order to determine the nature and impact of the incident.

The incident will be classified according to the table below:

Classification	Description	Action
High	A high-level incident possibly involving scenarios where the RZ KSK is lost or compromised.	If the incident is suspected to have compromised or lost the private key of any KSK, this Emergency KSK Rollover Plan will be executed.
Medium	A medium-level incident possibly involving the inability to perform operations within the required time. For example, inability to perform a KSK ceremony on time, Crypto Officers (CO) and/or Recovery Key Share Holders (RKSH) are unavailable.	If the incident delays the ability to perform the operations within the required time, the Disaster Recovery and Business Contingency Procedure will be enacted.
Low	A low-level incident possibly involving scenarios where an event will not impact the RZ KSK operation, system, property, or trust.	If the incident priority is low it will be addressed by RKOS according to the Incident Handling Procedure.

The scope, severity, and damage of any incident will be assessed and a remediation plan will be developed and implemented. The plan will also include mitigating measures to prevent recurrence of the event, according to the Incident Handling Procedure.

RKOS is responsible for the identification and resolution of incidents and security breaches. RKOS will report all incidents to the PMA. It is the responsibility of the PMA to decide whether the particular situation warrants executing the "Incident Handling Procedure", the "Disaster Recovery and Business Continuity Procedure" or the “Emergency KSK Rollover Plan”.

The “Incident Handling Procedure” and the “Disaster Recovery and Business Continuity Procedure” describe how the RZ KSK Operator is able to restore essential operations within 48 hours. These functions include:

- Communication with the RZ ZSK Operator, Trusted Community Representatives (TCRs), resolver operators, and the community at large
- Ability to import KSRs (Key Signing Requests) and export SKRs (Signed Key Responses)
- Generation of KSKs
- Processing and signing of KSR contents
- Publishing the Trust Anchor

5 Private Key Compromise Procedures

5.1 KSK Compromise

Upon the covert or overt compromise of a KSK, RKOS will assess the situation, develop an appropriate action plan, and implement the action plan with approval from the PMA and PTI executive management.

As part of the KSK emergency rollover procedures, the RZ KSK Operator maintains the capability of being able to generate and publish an interim Trust Anchor within 48 hours. In favorable circumstances, this interim Trust Anchor MAY be used to facilitate an orderly RFC 5011 automatic KSK rollover to a new Trust Anchor generated at a scheduled Key Ceremony held within 90 days.

If the previous Trust Anchor private key was compromised but not lost, the previous Trust Anchor MUST be revoked.

The RZ KSK Operator will inform the community of an emergency within 48 hours via the channels stipulated in the communication plan section.

5.2 KSK Loss

If the private component of a Trust Anchor is permanently lost, that loss will be detected no later than at the Key Ceremony when the key is supposed to be used. At that point in time, the RZ Maintainer will have signatures for at least 33 days of independent operations.

If possible, a Key Ceremony will be scheduled within 48 hours to generate a new KSK. If the RZ KSK Operator is unable to accommodate a Key Ceremony, an interim KSK MUST be generated by the RZ KSK Operator and published as a Trust Anchor within the stipulated 48 hours.

The community MUST be given a minimum of 30 days notice to add the new Trust Anchors to the validating resolvers before the Domain Name System Key (DNSKEY) resource record set (RRset) has to be re-signed with the new Trust Anchor. Failure to update a validating resolver will render that resolver inoperable.

The RZ KSK Operator MUST inform the community of an emergency as soon as possible via the channels stipulated in the communication plan section.

5.3 ZSK Compromise or Loss

The RZ KSK Operator will support Root Zone Zone Signing Key emergency rollover in the case of RZ ZSK compromise or Loss while following the RZ ZSK Operator's procedural directions.

6 Emergency KSK Rollover Procedure

The following procedure is for emergency rollover of the KSK:

1. The PMA Chair is notified by RKOS of an incident that MAY require an emergency rollover of the RZ KSK.
2. The PMA Chair MUST chair a PMA meeting to determine the impact of the incident, whether it would require an emergency rollover of the RZ KSK, and if the incident calls for immediate action or if it can be scheduled for a later date.
3. The PMA Chair MUST coordinate the execution of the communication plan.
4. The PMA Chair MUST notify the RZ ZSK Operator of the incident that would call for an RZ KSK rollover.
5. The PMA Chair MUST engage the RZ ZSK Operator to create a schedule of events for the rollover of the RZ KSK and move ahead with the plan.

6.1 Technical Steps for Emergency KSK Rollover

1. If the RZ KSK Operator is unable to accommodate a key ceremony within an acceptable time frame with respect to the urgency and impact of the incident, an interim KSK MUST be generated by the RZ KSK Operator using the best available means and published as a Trust Anchor within the stipulated 48 hours.
2. A Key Ceremony MUST be scheduled within 90 days where the new official Trust Anchor is generated and the DNSKEY RRsets required for the rollover are signed.
3. The RZ KSK Operator MUST collaborate with ICANN's Communications team to announce the rollover using the channels stipulated in the DPS as well as other modes of notification suggested by the communications team. An RFC 5011 automatic rollover MAY also be used if applicable.
4. When the required 30 days notice has elapsed, the ZSK Operator MAY start publishing a DNSKEY RRset using only the newly generated KSK as the Trust Anchor and if possible the old Trust Anchor will be marked as revoked.
    a. In the event of the private component of the old Trust Anchor is permanently lost, it will not be possible to mark the old Trust Anchor as revoked since the private key it is not available, and in turn it will be not possible use RFC 5011 (Automated Updates of DNSSEC Trust Anchors) and the new Trust Anchor SHOULD be added manually by the DNSSEC resolver operators.
5. The KSK rollover will be considered complete once the stakeholders (such as the Root Server Operators and Relying Parties) systems and processes are functioning as designed, at which point the RZ KSK Operator MAY destroy the private key of the previous Trust Anchor.

7 Communication Plan

Upon a KSK emergency rollover, the Practices Manager (PMA Chair) will work with the communications team to execute a response strategy according to the following response flow:

1. Assess Situation
    a. Review available information, seek additional information where necessary
2. Establish Response Strategy
    a. Develop messaging and content, and secure approvals
    b. Establish stakeholder outreach strategy
    c. Activate real-time media and social media monitoring
    d. Prep spokesperson(s)
3. Communicate
    a. Update community, board and organization, technical partners, ISPs and other relevant stakeholders
    b. Track and field inquiries from media/analysts/influencers
    c. Coordinate additional logistics (website, media briefings, etc.) as appropriate
4. Monitor and Refine
    a. Share regular updates, including media and social media monitoring reports
    b. Return to the first step if the situation escalates
5. Debrief and Analyze
    a. After the crisis is resolved, review response and learnings
    b. Update crisis plan with key learnings and apply to future incident response

8 Contact Information

Root Zone KSK Policy Management Authority
Public Technical Identifiers
12025 Waterfront Drive, Suite 300.
Los Angeles, CA 90094
USA
+1 (310) 823-9358 (voice)
+1 (310) 823-8649 (fax)
root-ksk-pma@icann.org

Appendix A: Acronyms

CO	Crypto Officer
DNSKEY	Domain Name System KEY
DNSSEC	Domain Name System Security Extensions
DPS	DNSSEC Practice Statement
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
KMF	Key Management Facility
KSK	Key Signing Key
KSR	Key Signing Request
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
RKSH	Recovery Key Share Holders
RRset	Resource Record Set
RZ	Root Zone
SKR	Signed Key Response
TCR	Trusted Community Representative
ZSK	Zone Signing Key

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 2: Added an Objective and Scope section.
- Section 3: Developed a Roles and Responsibilities section based on existing material.
- Section 4: Clarified the private key compromise procedures.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 1: Added definitions.
- Section 2: Added scenarios covered under this plan.
- Section 3: Added roles and responsibilities.
- Section 4: Added the incident management section.
- Section 6: Clarified if the private key of the KSK is permanently lost, it will be not possible to mark the Trust Anchor as revoked.
- Section 7: Added communication plan strategy.
- Updated Appendix A to reflect only the acronyms present in the document.

Revision 3.2 - 04 November 2020

- Annual review: Update version information and dates.
- Overall: Uniformly specified “Practices Manager” as “PMA Chair”.
- Section 4: Specified related PMA documents required for disaster recovery.
- Appendix A: Remove the DR acronym no longer used in the document.

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