Root Zone KSK Operator Disaster Recovery and Business Contingency Procedure

Version 3.3

Root Zone KSK Operator Policy Management Authority

04 November 2020

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).

In the context of RZ KSK operation, disruption is defined as the inability to perform operations within the required time. It does not include conditions under which operations can resume in sufficient time after a reasonable rescheduling or repair.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 (https://www.ietf.org/rfc/rfc2119.txt).

2 Objective and Scope

The objective for this procedure is to define requirements and recommendations for disaster recovery and business continuity procedures to be performed by designated personnel, systems, and other means.

There are three scenarios within the scope of this procedure:

- KSK Signing Disaster: Inability to produce a Signed Key Response (SKR) in a standard key ceremony using either site within the prescribed time window before the Resource Record Signature (RRSIG) on the Domain Name System KEY (DNSKEY) RRSIG expires due to unforeseen events beyond the control of the RZ KSK operator
- KSK Compromise Disaster: Disclosure of the private component of the KSK due to either exfiltration at either site, or through independent derivation of the private component
- Lost KSK Disaster: Inability to access the production KSK due to unrecoverable equipment or facility failure

3 Roles and Responsibilities

3.1 RZ KSK Operations Security

The RZ KSK Operations Security (RKOS) is responsible for the identification and resolution of incidents and security breaches in accordance with this procedure, including coordinating the actions to be performed relating to potential disaster recovery (DR) scenarios.

3.2 RZ KSK Operator Policy Management Authority

The RZ KSK Operator Policy Management Authority (PMA) is responsible for approving the disaster recovery procedures and to provide advice to operational staff and executive management during the invocation of disaster recovery procedures. As part of the same process, the PMA may advise on:

- Development of strategies to communicate with Trusted Community Representatives (TCRs), resolver operators, and with ICANN Communications team the general public
- Identification of the personnel who will perform the tasks
- Identification of the location where the DR operations will take place
- Determination of whether the Key Management Facilities (KMFs) are compromised or unavailable

4 Disaster Recovery Procedures

4.1 KSK Signing Disaster

An SKR needs to be generated to avoid an RRSIG expiration.

4.1.1 Key Management Facilities are unavailable

1. Communicate to COs the impending requirement to perform a Key Ceremony.
2. Film and create attestations for the event.
3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
4. Match the hashes, sign the Key Signing Request (KSR), and transmit the resultant SKR to the Root Zone Maintainer (RZM)
5. Publish the new KSK trust anchor in the RZ KSK Operator's repository and coordinate with ICANN's communications team if necessary.
6. Once at least one of the Key Management Facilities become available, schedule an extraordinary Key Ceremony to generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

4.1.2 Crypto Officers are unavailable

A. If at least one Key Management Facility is accessible:
    1. Communicate to COs the impending requirement to perform a Key Ceremony.
    2. Schedule an alternate date for the Key Ceremony if there is sufficient time before an RRSIG expiration, otherwise film and create attestations for the event and drill the safe deposit box if the materials are not accessible using physical keys. If time and circumstances permit, make arrangements with the COs to send their physical keys to the RZ KSK Operator in advance whilst preserving the chain of custody (such as with the use of tamper-evident packaging, couriers, and attestations).
    3. Match the hashes, sign the KSR, and transmit the resultant SKR to RZM.
    4. Once the minimum amount of COs, as defined by the DPS, become available to attend in person, schedule an extraordinary Key Ceremony to sign a new KSR, distribute new keys for the safe deposit box, then transmit the resultant SKR to the RZM.

B. If no Key Management Facilities are accessible:
    1. Communicate to COs the impending requirement to perform a key ceremony.

2. Film and create attestations for the event.
3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
5. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
6. Once the Key Management Facility becomes available and the minimum amount of COs, as defined by the DPS, are available to attend in person, schedule an extraordinary Key Ceremony to generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

4.1.3 High risk of prolonged unavailability of necessary personnel or facilities

1. Make an assessment, using expert opinion where possible, of the duration of the likely impairment to normal KSK operations.
2. Communicate with COs the requirement to generate additional RRSIGs to span an extended period of signing the root zone.
3. Formulate a plan to determine how the additional RRSIGs should be generated and present the plan to ICANN and PTI executive management for approval, whilst notifying the PMA.
4. Coordinate with RZM to generate additional KSRs to be signed at the next ceremony.
5. Perform a key signing ceremony to generate the additional RRSIGs.
6. Securely store additional RRSIGs until they are transmitted to RZM.
7. Provide RRSIGs to RZM as they are needed in accordance with the KSK Operator's DPS.

4.2 KSK Compromise Disaster

The SKR needs to be generated to avoid an RRSIG expiration, but the KSK has been compromised by means of exfiltration or derivation.

4.2.1 Crypto Officers are available to attend in person

A. At least one Key Management Facility is available
    1. Communicate to COs the impending requirement to perform a Key Ceremony.
    2. Determine which algorithm and key length SHOULD be used.
    3. Film and create attestations for the event.
    4. Destroy the existing KSK if possible.
    5. Generate a new KSK in another HSM. Use a KSK generation script as reference.
    6. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
    7. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
    8. Replace and secure all compromised hardware as soon as possible.

B. Key Management Facilities are NOT available

1. Communicate to COs the impending requirement to perform a Key Ceremony.
2. Film and create attestations for the event.
3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
5. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary for broader announcement.
6. Once the Key Management Facility becomes available, schedule an extraordinary Key Ceremony to replace all compromised HSMs, generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

4.2.2 Crypto Officers are NOT available to attend in person

A. At least one Key Management Facility is available

1. Communicate to COs the impending requirement to perform a Key Ceremony.
2. Schedule an alternate date for the Key Ceremony if there is sufficient time before RRSIG expiration, otherwise film and create attestations for the event and drill the safe deposit box if the materials are not accessible using physical keys.
3. Destroy the existing KSK if possible.
4. Generate a temporary KSK in a new HSM. Use a KSK generation script as reference.
5. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
6. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary for broader announcement.
7. Schedule an extraordinary Key Ceremony to replace all compromised HSMs, generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

B. Key Management Facilities are NOT available

1. Communicate to COs the impending requirement to perform a Key Ceremony.
2. Film and create attestations for the event.
3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
5. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
6. Once the Key Management Facility becomes available, and the minimum amount of COs, as defined by the DPS, are available to attend in person, schedule an extraordinary Key Ceremony to generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

4.3 Lost KSK Disaster

An SKR needs to be generated to avoid an RRSIG expiration, but the KSK is not accessible due to failure on all HSMs.

4.3.1 Recovery Key Share Holders and Crypto Officers are available in person

A. At least one Key Management Facility is available and KSK backup is available
    1. Communicate to COs and Recovery Key Share Holders (RKSHs) the impending requirement to perform a Key Ceremony.
    2. Film and create attestations for the event.
    3. Reconstruct the existing KSK in another HSM using encrypted backup and RKSH credentials.
    4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
B. At least one Key Management Facility is available and KSK backup is NOT available
    1. Communicate to COs and RKSHs the impending requirement to perform a Key Ceremony.
    2. Film and create attestations for the event.
    3. Generate a new KSK in a new HSM. Use a KSK generation script as reference.
    4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
    5. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
C. Key Management Facilities are NOT available (KSK backup is NOT available)
    1. Communicate to COs and RKSHs the impending requirement to perform a Key Ceremony.
    2. Film and create attestations for the event.
    3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
    4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
    5. Publish the temporary KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary for broader announcement.
    6. Once the Key Management Facility becomes available, schedule an extraordinary Key Ceremony to generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

4.3.2 Recovery Key Share Holders are NOT available

This procedure is applicable whether or not COs are available.

A. At least one Key Management Facility is available

1. Communicate to all COs and RKSHs the impending requirement to perform a Key Ceremony.
2. Film and create attestations for the event.
3. Generate a temporary KSK in a new HSM. Use a KSK generation script as reference.
4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
5. Publish the temporary KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
6. Once all RKSH becomes available, schedule an extraordinary Key Ceremony to distribute appropriate credentials.

B. Key Management Facilities are NOT available

1. Communicate to COs the impending requirement to perform a Key Ceremony.
2. Film and create attestations for the event.
3. Generate a temporary KSK in another HSM outside of the Key Management Facility. Use a KSK generation script as reference.
4. Match the hashes, sign the KSR, and transmit the resultant SKR to the RZM.
5. Publish the new KSK trust anchor in the RZ KSK Operator's repository. Coordinate with ICANN's communications team if necessary.
6. Once a Key Management Facility becomes available, schedule an extraordinary Key Ceremony to generate a new KSK and SKR, distribute credentials, then execute RFC 5011 KSK rollover if possible.

Appendix A: Acronyms

CA	Ceremony Administrator
CO	Crypto Officer
DNSKEY	Domain Name System KEY
DPS	DNSSEC Practice Statement
DR	Disaster Recovery
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
IW	Internal Witness
KMF	Key Management Facility
KSK	Key Signing Key
KSR	Key Signing Request
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
RRSIG	Resource Record Signature
RZ	Root Zone
RZM	Root Zone Maintainer
SA	System Administrator
SKR	Signed Key Response
SSC	Safe Security Controller
TCR	Trusted Community Representative

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.
- Changed the title from "Plan" to "Procedure" to reflect the current contents of the document.
- Section 1: Clarified the definition of "disruption".
- Section 2: Added an Objective and Scope section. Clarified that the document's scope is three disaster scenarios. Defined the document's objective.
- Section 3: Moved the text about roles and responsibilities to be under a new Section 3, Roles and Responsibilities heading.
- Section 4: Renamed the section and its major subsections to correspond to the three disaster scenarios listed in Section 2.

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 3: Clarified the PMA decision

Revision 3.2 - 07 April 2020

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 2: Updated definitions of disasters
- Section 3: Clarified responsibilities for roles
- Section 4: Updated definitions of scenarios, new scenario for extended signing period

Revision 3.3 - 04 November 2020

- Annual review: Update version information and dates.
- Made minor formatting changes.
- Section 4.1.3: Added step to secure additional RRSIGs. Specified required management approval level for disaster recovery operations.