Root Zone KSK Operator Key Management Procedure

Version 3.7

Root Zone KSK Operator Policy Management Authority

15 March 2024

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 Internet Corporation for Assigned Names and Numbers (ICANN).

All cryptographic operations involving the RZ KSK are conducted within physically protected environments known as Key Management Facilities (KMFs) that deter, prevent, and detect any unauthorized use of, access to, or disclosure of sensitive information and systems, whether covert or overt. The purpose of this procedure is to help ensure that any risks associated with the management of cryptographic keys are properly mitigated to an acceptable level, and that this level of risk is managed and maintained over time.

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 key management procedures to be performed by designated personnel, systems, and other means.

3 Roles and Responsibilities

3.1 Assignment of Ceremony Administrator

The President of PTI or RZ KSK Operations Security (RKOS) is responsible for assigning a Ceremony Administrator (CA) for each upcoming ceremony and requesting sufficient resources to be made available at the executive level to support the ceremony.

3.2 Ceremony Administrator

The Ceremony Administrator (CA) for a specified ceremony is responsible for its execution as described in sections 5 and 6 of this document. The CA holds the guard key to all safe deposit boxes contained within the Credentials Safe (see section 3.3). The CA is responsible for storing the guard key in a safe place. The guard key, in combination with each Crypto Officer's (CO's) tenant safe deposit box key, is REQUIRED to open any of the COs' safe deposit boxes. The CA is a trusted role performed by an appointed and trained staff member.

For facility access, the CA MAY access tiers one (1) through three (3) alone, and MUST be accompanied by an Internal Witness (IW) when accessing the Key Ceremony Room (Tier 4) or the Safe Room (Tier 5).

The CA MAY be granted physical access to the secure offsite backup facility where copies of the audit log information are stored.

At least two (2) CAs are REQUIRED per KMF. An individual CA MAY serve multiple KMFs if required.

3.3 Safe Security Controller

The Safe Security Controllers (SSCs) are trusted roles that hold the combinations for the Equipment Safes containing the Hardware Security Module (HSM) and the Credential Safes containing the COs' safe deposit boxes. The combination codes are kept confidential by the respective SSCs.

There are two (2) SSC roles:

- Safe Security Controller 1 (SSC1) holds the combination to Safe 1 (Equipment Safe).
- Safe Security Controller 2 (SSC2) holds the combination to Safe 2 (Credentials Safe).

For facility access, each SSC MUST be escorted by the CA and IW to the Safe Room (Tier 5).

Two (2) SSCs per safe are REQUIRED per KMF, giving a total of four (4) persons per KMF. A person serving as an SSC1 MUST NOT serve as an SSC2 and vice versa. An SSC MUST NOT serve multiple KMFs. Replacement of an SSC REQUIRES a change in combination for the corresponding safe to maintain confidentiality.

3.4 System Administrator

The System Administrator (SA) is a support role with the competence of resolving sudden problems arising from technical failures of the equipment required at the Key Ceremony, e.g., access control system (ACS), audiovisual equipment, computer equipment, HSM, cabling, and the heating, ventilation, and air conditioning (HVAC) system. SA is a trusted role performed by appointed and trained staff.

The SA MAY escort unauthorized people, e.g., COs, SSCs, maintenance personnel, and external witnesses within the KMF.

The SA is responsible for holding and maintaining the codes required for programming of the ACS and intrusion detection system (IDS). These codes are kept confidential to the SA role.

For facility access, the SA MAY access tiers one (1) through three (3) alone, and is REQUIRED to be accompanied by an IW for Key Ceremony Room (Tier 4) access. The SA does not have access to the Safe Room (Tier 5), so the SA MUST be escorted into the Safe Room (Tier 5) by both CA and IW.

At least two (2) SAs are REQUIRED per KMF. An individual SA MAY serve multiple KMFs if required.

3.5 Internal Witness

The Internal Witness (IW) is a trusted role performed by appointed and trained staff. The IW observes the Key Ceremony and attests that it has been executed as described in the Key Ceremony procedures (see sections 5 and 6). In order to comply with the dual occupancy requirement (see Section 4.6), multiple IWs MAY be required during a single Key Ceremony.

For facility access, the IW MAY access tiers one (1) through three (3) alone, is REQUIRED to be accompanied by a CA or SA for Key Ceremony Room (Tier 4) access, and is REQUIRED to be accompanied by a CA for Safe Room (Tier 5) access.

At least two (2) IWs are REQUIRED per KMF. An individual IW MAY serve multiple KMFs as required.

3.6 External Witness

The External Witnesses (EWs) observe the Key Ceremony and attest that it has been executed as described in the Key Ceremony procedures (see sections 5 and 6). EWs are not affiliated with PTI or ICANN. An auditor is considered to be an EW in this context.

EW is not a trusted role and does not have access to any tier inside the KMF. Escort is REQUIRED at all times.

3.7 Staff Witness

The Staff Witnesses (SWs) observe the Key Ceremony and attest that it has been executed as described in the Key Ceremony procedures (see sections 5 and 6). SWs are affiliated with PTI or ICANN.

SW is not a trusted role and does not have access to any tier inside the KMF. Escort is REQUIRED at all times.

3.8 Crypto Officer

A Crypto Officer (CO) holds a key to a safe deposit box placed inside Safe 2 (Credentials Safe). The CO is responsible for handling and safely storing the key between Key Ceremonies. Each safe deposit box contains the credentials (in tamper-evident packaging) required for the corresponding CO to authorize operations performed with the HSM.

COs are Trusted Community Representatives (TCRs), representing the technical Internet community, and are not affiliated with PTI, ICANN, or Verisign. The TCRs are not contractually bound to fulfill their duties to the RZ KSK Operator.

The CO is not granted access to any tier inside the KMF; escort is REQUIRED at all times.

Seven (7) COs are REQUIRED per KMF. An individual CO MUST NOT serve multiple KMFs.

3.9 Recovery Key Share Holder

Each Recovery Key Share Holder (RKSH) is the custodian of one of the seven (7) key shares of the Storage Master Key (SMK), the Domain Key, and the CO key. Each key share is kept by an individual RKSH in a bank safe deposit box or similar secure storage facility in a location convenient for the RKSH. Each SMK share is stored in a smartcard or iKey placed inside tamper-evident packaging.

The RKSH is responsible for providing and maintaining records of where the shares are stored, and participating in an annual inventory providing proof of possession of their key shares. RKSHs are TCRs, representing the technical Internet community, and are not affiliated with PTI, ICANN, or Verisign. The TCRs are not contractually bound to fulfill their duties to the RZ KSK Operator.

The RKSH is not granted physical access to any tier inside the KMF. Escort is REQUIRED at all times.

Seven (7) RKSHs in total are REQUIRED and are shared by all KMFs.

4 General Ceremony Provisions

4.1 Ceremony Initiation

The CA is responsible for initiating all ceremonies.

4.2 Ceremony Attendees

The RKOS is responsible for coordinating the ceremony attendees. See section 11 for details on how many participants from each role will be required for each ceremony.

4.3 Pre-Ceremony Actions

Before the ceremony is executed, the RKOS MUST prepare the scripts to be followed at the ceremony. Multiple types of ceremonies MAY be executed together at a single event. The exact subprocedures required for each ceremony are specified in the scripts.

4.4 Post-Ceremony Actions

After a ceremony has been executed, the CA or RKOS MUST collect any output which should be exported from the ceremony, place each component in a sealed, tamper-evident bag under the supervision of an IW, and bring it from the KMF to the respective destination.

The CA or RKOS also MUST make copies of the ceremony output under the supervision of the IW participating at the Key Ceremony. The copies MUST be archived at an offsite storage facility.

4.5 Key Distribution

Key distribution is REQUIRED to occur promptly after each Key Generation Ceremony. It MUST be completed before any key is taken into its Operational Period.

The RKOS MUST ensure that the key material has arrived at each KMF, is safely stored in the equipment safe, and the chain of custody was not broken before the keying material is taken into its Operational Period.

A courier is responsible for maintaining custody of the assigned package and keeping it in a safe place throughout the entire key distribution process, from retrieval to deposit, which SHOULD be completed as quickly as possible.

Each package with keying material MUST be initialed by all participating couriers. The couriers SHOULD NOT travel together as a group during transportation. A courier MUST be a Trusted Person with an active role.

Upon arrival at the destination facility, the tamper-evident bags MUST be verified by all couriers as evidence of the confidentiality of the keying material being maintained during key distribution.

4.6 Dual Occupancy

Access to the Key Ceremony Room (Tier 4) and Safe Room (Tier 5) is subject to enforcement of dual occupancy of authorized persons, i.e. the same rules apply for occupancy as for entry.

5 Key Management Ceremonies

Key Management Ceremonies are ceremonies that involve activation of an HSM. HSM activation MUST require 3 of 7 shares assigned solely to COs. If applicable, this may be enforced by employing additional protection layers within the HSM requiring credentials solely assigned to COs.

The ceremonies are designed to be executed in the listed order, but components not applicable for a given ceremony MAY be skipped by the CA.

The necessary steps for each role in each module MUST be documented in detail in the Key Ceremony script.

5.1 Key Management Ceremonies Prologue

Before any other Key Management action can be executed, CO credentials and HSMs MUST be extracted from their respective safes and placed into the Key Ceremony Room (Tier 4).

5.2 HSM Initialization

A newly commissioned HSM MUST be initialized before use. As part of the initialization process, HSMs MUST be configured to require existing CO credentials, and encryption keys used for HSM backup MUST be initialized. The HSM is REQUIRED to pass the acceptance test as described in section 6.14 "Equipment Acceptance Testing" before initialization.

5.2.1 All HSMs

The ceremony script for HSM initialization MUST describe the following steps for all HSMs being initialized:

1. Verify HSM hardware integrity by checking the serial number of the tamper-evident bag and the serial number against the log records from the acceptance test.
2. For Keyper HSMs, import the Adapter Authorization Key (AAK) to authorize CO credentials and perform basic HSM configuration. For Thales Luna HSMs, reuse the existing credential sets during initial configuration to ensure interoperability with other Thales Luna production hardware.
3. For Keyper HSMs, import the SMK and Application Key backup. For Thales Luna HSMs, import the key backup from a Thales Luna Backup HSM configured with the same Domain and CO Keys.
4. Sign a duplicate copy of the ceremony's Key Signing Request (KSR) to ensure HSM functionality and CO credential operation.

5.2.2 First HSM sharing a Recovery Key

All HSMs sharing the same set of RKSHs share the same SMK, or Domain and CO Keys. The SMK or Domain and CO Keys are REQUIRED to be generated, distributed, and installed in all HSMs in the system prior to any of the HSMs being taken into production.

The ceremony script for SMK generation and distribution MUST describe the following steps for all HSMs being initialized:

1. Generate the SMK, or Domain and CO Keys.
2. Split and export two (2) sets of Recovery Key Shares.
3. Reassemble and install the SMK, or Domain and CO Keys in the other HSMs at the same KMF.
4. Store Recovery Key Shares in tamper-evident bags. Two full sets of Recovery Key Shares MUST be stored in a tamper-evident bag.
5. Distribute Recovery Key Shares to RKSHs.

6. Reassemble and install the SMK or Domain and CO Key shares at each other KMF which will be used for production.

5.3 HSM Decommission

The decommissioning procedure is REQUIRED to ensure with reasonable certainty that all private keys and crypto parameters on which the Trust Anchor depends are destroyed. The ceremony script for HSM decommissioning MUST include the following steps:

1. Zeroize and tamper the HSM.
2. Verify the HSM has been reset.
3. Optionally, destroy the HSM.

5.4 Key Generation

Key generation is split into two phases: phase 1 is executed at the KMF where the key is generated, and phase 2 is executed at every other KMF. After phase 1 has been executed, two (2) copies of the application data (keys and associated data encrypted with the SMK or Domain and CO Keys) MUST be promptly transported to every other KMF and deposited as described in section 6.12 "Media Deposit" until phase 2 is to be executed. Phase 2 is normally executed together with another scheduled Key Management Ceremony, e.g., key signing.

5.4.1 Phase 1

The ceremony script for phase 1 of key generation MUST include the following steps:

1. Generate a new key in HSM 1:
    a. Activate HSM 1.
    b. Generate the new key.
    c. Announce the generated key's fingerprint (hash) to participating witnesses.
    d. Export the public key component onto at least portable media.
    e. Back up the application data to two (2) pieces of portable media or backup HSMs for every KMF, including the KMF used for key generation.
    f. Deactivate HSM 1.
2. Repeat the restoration process of the new key onto every other HSM onsite:
    a. Activate the HSM.
    b. Restore the application data backup onto the HSM.
    c. Deactivate the HSM.
3. Store two (2) copies of the application data backup in the equipment safe onsite.
4. Temporarily store, transport, and deposit the two copies of the application data backup or two backup HSMs for each other KMF which will be used for production.

5.4.2 Phase 2

The ceremony script for phase 2 of key generation MUST include the following steps:

1. Retrieve and authenticate the application data backup or backup HSMs stored in the equipment safe.
2. Restore the new application data onto each HSM:
    a. Activate the HSM.
    b. Restore the application data backup onto the HSM.
    c. Deactivate the HSM.
3. Place the application data backup or backup HSM in the equipment safe onsite.

5.5 Key Signing

The RZ KSK Operator MUST provide the RZ Zone Signing Key (ZSK) Operator with a signed and valid Domain Name System Security Extensions (DNSSEC) resource record set (RRset) for the RZ ZSK Operator's current keys and the public component of the KSKs.

5.5.1 Signing Practice

The signing practice of the RZ is divided into quarterly continuous time cycles of approximately 90 days. Time cycles begin on the following dates each year:

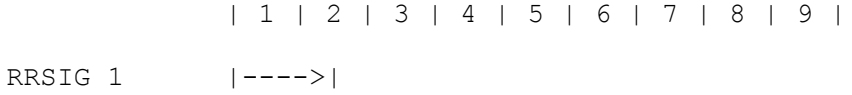
- January 1st
- April 1st
- July 1st
- October 1st

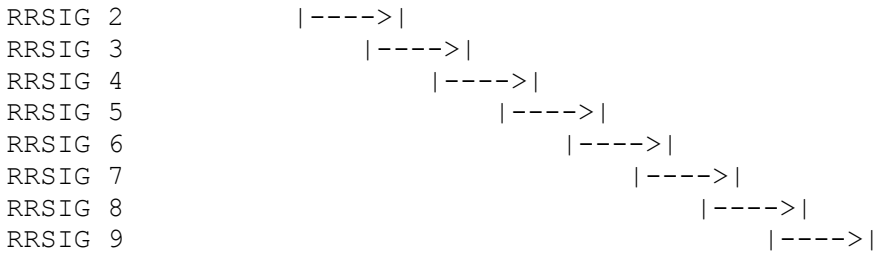
For each of these time cycles, the RKOS MUST schedule a Key Ceremony in the prior calendar quarter, but no later than 33 days before the time cycle commences. At this Key Ceremony, all of the necessary RZ KSK operations MUST be performed to enable the RZ Maintainer to operate and publish the zone independently throughout the period.

To facilitate automatic updates of resolvers' Trust Anchors as described in RFC 5011, while minimizing the number of concurrent keys in the root key set, each of the 90-day time cycles is divided into 10-day slots (nine slots).

A time cycle will never last less than 90 days. If the time cycle is more than 90 days, the last slot in the cycle is expanded to fill the period.

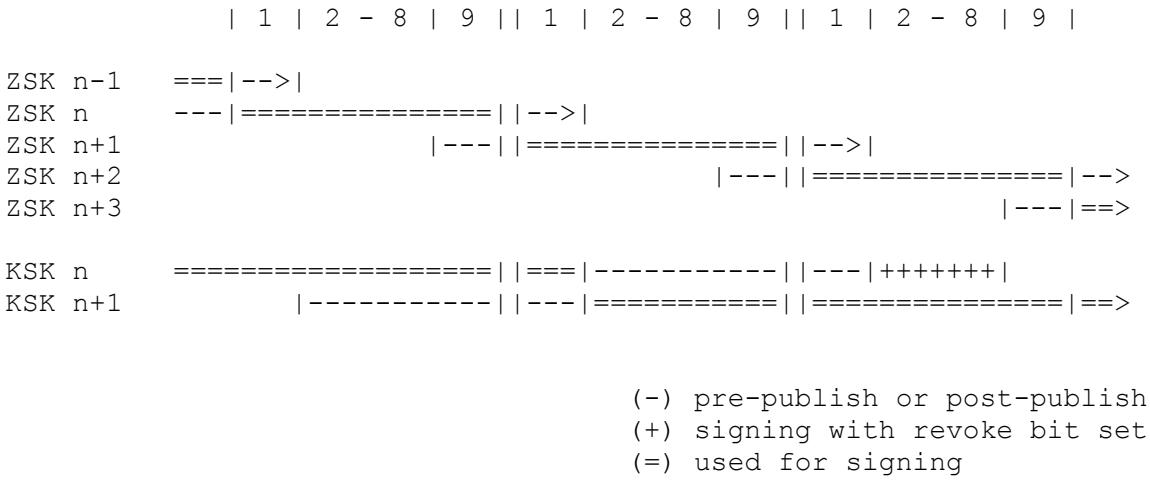
For each of these slots, there is a pre-generated Domain Name System Key (DNSKEY) key set that is signed at the Key Ceremony with 21 days’ validity time to allow for signature overlap. The RZ Maintainer MUST select the current key set and publish it with the corresponding valid signature.





DNSKEY RRSIG's validity period within the cycle

The Root Zone Maintainer may use slots at the edges of every time cycle for pre-publishing and post-publishing of RZ ZSK rollovers.



Idealized 270 day cycle of ZSK rollovers with critical phases of a KSK rollover

In the event of an RZ KSK rollover and RZ ZSK rollovers in the same cycle, time slots are used for pre-publishing, post-publishing, adding, and deleting Trust Anchors in the following order:

RZ KSK Pre-Publication

Slot 1: publish ZSK (n) + ZSK (n-1) + KSK (n), sign DNSKEY RRset with KSK (n)
Slot 2-8: publish ZSK (n) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n)
Slot 9: publish ZSK (n) + ZSK (n+1) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n)

RZ KSK Rollover

Slot 1: publish ZSK (n) + ZSK (n+1) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n)
Slot 2-8: publish ZSK (n+1) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n+1)

Slot 9: publish ZSK (n+1) + ZSK (n+2) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n+1)

RZ KSK Revocation

Slot 1: publish ZSK (n+1) + ZSK (n+2) + KSK (n) + KSK (n+1), sign DNSKEY RRset with KSK (n+1)
Slot 2-8: publish ZSK (n+2) + KSK (n+1) + revoke KSK (n), sign DNSKEY RRset with revoke KSK (n) + KSK (n+1)
Slot 9: publish ZSK (n+2) + ZSK (n+3) + KSK (n+1), sign DNSKEY RRset with KSK (n+1)

At each publication, the Root Zone Maintainer selects and includes the current key set and corresponding signature(s), and then signs all other authoritative records within the root zone using the current RZ ZSK. In this way, all phases of the KSK rollover can be postponed or reverted up until the revocation phase.

5.5.2 KSR Processing

The RZ Maintainer MUST select and include the current key set and corresponding signature(s), and then sign all other authoritative records within the root zone using the current RZ ZSK. The RKOS MUST maintain contact with the RZ ZSK Operators technical staff to ensure the timely reception of the KSR.

The RKOS, in all cases, as part of the Key Ceremony preparations MUST generate a SHA-256 hash of the KSR document, and using an out-of-band method (verbally over the phone, by fax, or any other available method), verify the authenticity and integrity of the KSR document before entering it into the signer system.

After the Key Ceremony, the Signed Key Response (SKR) MUST be provided to the RZ ZSK Operator. The KSR/SKR MAY be exchanged in any way the RKOS determines to be suitable with respect to the situation, and which provides reasonable protection from public exposure, errors, and substitution.

In the event disaster recovery procedures have been activated resulting in the generation of additional SKRs designated for future validity periods, the RZ KSK Operator must withhold and securely store these SKRs until they are transmitted to the RZ ZSK Operator. The storage method must reasonably safeguard the confidentiality, integrity, and availability of additional SKRs by utilizing the KMF and an offsite storage facility. Physical copies MUST be secured in tamper-evident bags in locations only RKOS and authorized Trusted Persons may access. Any digital copies MUST be encrypted using a known strong cipher and stored in secure computer systems only RKOS and authorized Trusted Persons may access.

Each key set within the KSR is REQUIRED to be self-signed with the active key to provide proof of possession of the corresponding private key. The signer system MUST automatically validate this signature, perform checking of available key parameters, and validate any available proof traceable to the previous KSR before accepting the KSR for signing.

If proof traceable to the previous KSR is not available, the RKOS MUST perform an out-of-band verification (verbally over the phone, by fax, or any other available method) from a known source to ensure the authenticity and integrity of the KSR document before overriding the automatic checking of the signer system.

The ceremony script for key signing/KSR processing MUST include the following steps:

1. Activate the HSM.
2. Import the KSR from portable media.
3. Validate the KSR data.
4. Verify KSR integrity through either of the following methods:
    a. Establishing contact with a representative of the RZ ZSK Operator (over a loudspeaker phone or appearing in person), known to the participants at the Key Ceremony, and verifying the integrity and authenticity of the KSR data by having that representative read the hash
    b. Automatically (using the signer system) verifying proof traceable to the last KSR sent by the RZ ZSK Operator.
5. Process (sign) the KSR and produce the corresponding SKR.
6. Export SKR data to portable media.
7. Deactivate the HSM.

5.6 Private Key Destruction

After the Operational Period of an RZ KSK has ended, it MUST be retained for at least 30 days. After the 30 days of retention, it expires and SHOULD be destroyed at the earliest convenience, which need not be simultaneous for all KMFs. It is RECOMMENDED that key destruction is planned for as part of the regular Key Signing Ceremonies at each KMF.

The ceremony script MUST include the following steps:

1. Activate the HSM.
2. Delete the key from the HSM.
3. Verify the key no longer exists in the HSM.
4. Create new backups containing only the current keys (if necessary).
5. Destroy any backups containing the expired keys.
6. Deactivate the HSM.

5.7 Key Management Ceremonies Epilogue

After any key management action has been executed, and before the participants can leave, all equipment and CO credentials MUST be placed in signed and sealed tamper-evident bags and safely stored into their respective containers in the Safe Room (Tier 5).

6 Administrative Ceremonies

Administrative Ceremonies include all ceremonies that do not require activation of an HSM. These activities may be performed ad hoc, combined with other administrative activities, or included in a Key Ceremony.

6.1 SSC Enrollment

An SSC enrollment MUST be conducted at a ceremony at the appointed KMF. The ceremony for an SSC enrollment MUST be administered by the CA and witnessed in person by an IW. The ceremony script for an SSC enrollment MUST include the following steps:

1. Open the already-unlocked safe (SSC).
2. Select and set a new combination code (SSC).
3. Verify the new combination code (SSC).
4. Update and sign the audit log and safe log (SSC).
5. Close and lock the safe (SSC).
6. Verify that the safe is locked (CA and IW).

At least one of the SSCs MUST attend. The non-attending SSC MAY receive the new combination code from the attending SSC.

6.2 SSC Replacement

An SSC replacement MUST be conducted at a ceremony at the appointed KMF. The ceremony for an SSC replacement MUST be administered by the CA and witnessed in person by an IW. The ceremony script for an SSC replacement MUST include the following steps:

1. Unlock and open the safe (resigning or remaining SSC).
2. Select and set the new combination code (remaining or new SSC).
3. Verify the new combination code (remaining or new SSC).
4. Verify the safe is locked (CA and IW).
5. Unlock and open the safe (remaining or new SSC).
6. Update and sign the audit log and safe log (resigning, remaining, and new SSC).
7. Close and lock the safe (remaining or new SSC).
8. Verify that the safe is locked (CA and IW).

At least one of the SSCs MUST attend. The non-attending SSC MAY receive the new combination code from the attending SSC.

6.3 SSC Combination Recovery

If the combination of a safe is lost, a new SSC(s) for the safe MAY be enrolled. In either case the safe MUST be forced open. The ceremony for an SSC combination recovery MUST be administered by the CA and witnessed in person by an IW. The ceremony script for an SSC combination recovery MUST include the following steps:

1. Force the safe open.
2. Verify the safe contents.
3. Update and sign the audit log and safe log.
4. Replace/repair the lock mechanism and/or safe door.
5. Enroll the SSC(s) (if required) as described in section 6.1.

6.4 CO Enrollment

A CO enrollment MUST be conducted at a ceremony at the appointed KMF. The ceremony for a CO enrollment MUST be administered by the CA and witnessed in person by an IW. The ceremony script for a CO enrollment MUST include the following steps:

1. Distribute two (2) tenant safe deposit box keys to CO (CA).
2. Open the safe deposit box using the first tenant key (CO together with CA using the guard key).
3. Verify the safe deposit box is empty (CO).
4. Close the safe deposit box (CO).
5. Open the safe deposit box (together with CA using the guard key) using the second tenant key (CO and CA).
6. Update and sign the audit log and safe log (CO).
7. Close the safe deposit box (CO).

6.5 CO Replacement

A CO replacement MUST be conducted at a ceremony at the appointed KMF. The ceremony for a CO replacement MUST be administered by the CA and witnessed in person by an IW. The ceremony script for a CO replacement MUST include the following steps:

1. Open the safe deposit box (resigning CO together with CA holding the guard key).
2. Verify the safe deposit box contents (resigning and new CO).
3. Replace the safe deposit box lock, or schedule the resigning CO's lock for replacement if a vacant safe deposit box is assigned to the new CO.
4. Distribute two (2) new tenant safe deposit box keys to the new CO (CA).
5. Open the safe deposit box using the first tenant key (new CO together with CA using the guard key).
6. Close the safe deposit box (new CO).
7. Open the safe deposit box using the second tenant key (new CO together with CA using the guard key).
8. Update and sign the audit log and safe log (new CO).

9. Close and lock the safe deposit box (new CO).

6.6 CO Tenant Key Unavailability Recovery

If a CO's tenant key is unavailable, a CO tenant key unavailability recovery MUST be conducted at a ceremony at the appointed KMF. The ceremony for a CO tenant key unavailability recovery MUST be administered by the CA and witnessed in person by an IW. The ceremony script for a CO tenant key unavailability recovery MUST include the following steps:

1. Force the safe deposit box open.
2. Verify the safe deposit box contents.
3. Replace the safe deposit box lock assembly or assign a new safe deposit box.
4. Enroll a new CO if required as described in section 6.4.

6.7 CO Tenant Key Disclosure Recovery

If a CO's tenant key is known to or has been potentially disclosed, a CO tenant key disclosure recovery MUST be conducted at a ceremony at the appointed KMF. The ceremony for a CO tenant key disclosure recovery MUST be administered by the CA and witnessed in person by an IW. The ceremony script for a CO tenant key disclosure recovery MUST include the following steps:

1. Open the CO's safe deposit box.
2. Verify the safe deposit box contents.
3. Replace the safe deposit box lock assembly or assign the CO a vacant safe deposit box, migrate the safe deposit box contents, and schedule the old lock for replacement.

6.8 Safe Deposit Box Lock Programming

Safe deposit box lock mechanisms MUST be programmed and thoroughly tested prior to introduction. This work MUST be performed at a ceremony in a KMF. A ceremony for safe deposit box lock programming MUST be administered by the CA and witnessed in person by an IW. The ceremony script for safe deposit box lock programming MUST include the following steps:

1. Inspect new lock assemblies for damage or evidence of tampering.
2. Program the guard key lock using the desired guard key (guard keys differ per KMF).
3. Ensure proper lock assembly operation testing both tenant keys and the guard key.
4. Place individual lock assemblies in tamper-evident bags.

6.9 RKSH Replacement

This ceremony MAY be scheduled at the most convenient location with respect to the resigning and new RKSHs, and it is not required to be performed within a KMF. However, it MUST be administered by the CA and witnessed in person by an IW. External witnesses (EW) or another TCR MAY also witness the ceremony.

1. Provide the Recovery Key Shares in tamper-evident bags (resigning RKSH).

2. Check the serial numbers of the tamper-evident bags containing the Recovery Key Shares (CA and IW).
3. Hand over the Recovery Key Shares to the new RKSH (CA and IW).
4. Verify that the tamper-evident bag has not been tampered with (new RKSH).
5. The tamper-evident bags SHOULD be replaced at the time of the RKSH replacement if the tamper-evident bags have visible wear or known vulnerabilities.

6.10 Unavailable RKSH Credential Recovery

If an RKSH or their associated recovery key share is known to be unavailable, a recovery procedure MUST be conducted as soon as possible. Reasonable efforts MUST be made to contact the RKSH through all known available means to determine the status of the RKSH and their recovery key shares. Each RKSH should designate an emergency contact to support this process.

If an RKSH is no longer available to perform their duties, reasonable efforts MUST be made to recover the RKSH's recovery key shares and return them to a Trusted Person. If the recovery key shares are returned, the recovery key shares should be inspected for tamper evidence in a secure ceremony environment. If there is insufficient evidence the chain-of-custody has been preserved (i.e. that tampering could have taken place), the recovery key shares SHOULD be considered compromised. Returned recovery key shares with no signs of tampering are eligible to be reassigned to a new RKSH.

If an RKSH is no longer able to access their recovery key shares, the recovery key shares should be considered lost.

6.11 Issuing of New Recovery Key Shares

This procedure includes generating and distributing new sets of Storage Master Key (SMK) Shares, or Domain and CO Key shares to all RKSHs. The new Recovery Key or Domain and CO Keys MUST be imported to all HSMs sharing the Recovery Key, typically all HSMs at all KMFs.

More information about Recovery Key generation and distribution can be found in section 5.2 "HSM Initialization".

NOTE: This ceremony is a Key Management Ceremony, since it requires HSMs to be activated, and is listed here for completeness only.

NOTE: All RKSHs and seven (7) COs per KMF, MUST attend because a new set of Recovery Key Shares are generated and distributed as part of this procedure.

6.12 Media Deposit

An Application Key Backup MUST be deposited in Safe 1 (Equipment Safe) for use at a future Key Management Ceremony or pending transport to another KMF. Media deposited MAY be extracted later as described in section "6.13 Media Extraction". The script for that ceremony MUST include the following steps:

1. Open Safe 1 (Equipment Safe) (SSC)
2. Deposit Media (CA)
3. Close Safe 1 (Equipment Safe) (SSC)
4. Verify that the safe is locked (CA and IW)

6.13 Media Extraction

An Application Key Backup previously placed into Safe 1 (Equipment Safe), as described in section 6.12 "Media Deposit", MAY be extracted for transportation to another KMF. The script for that ceremony MUST include the following steps:

1. Open Safe 1 (Equipment Safe) (SSC)
2. Extract Media (CA)
3. Close Safe 1 (Equipment Safe) (SSC)
4. Verify that the safe is locked (CA and IW)

6.14 Equipment Acceptance Testing

Acceptance testing of new equipment MUST be performed in the Key Ceremony Room (Tier 4) and witnessed by a CA or IW, and MAY include an SA.

HSM hardware MUST include verification of its serial number and the integrity of the tamper-evident bag in which the device was shipped. The serial number and tamper-evident bag number should be compared against the out-of-band information provided by the manufacturer. If applicable, HSM hardware SHOULD be additionally verified using additional protection layers.

After the testing has been completed successfully, the equipment MUST be stored in tamper-evident packaging, noting the serial numbers of the packaging in the log and storing the equipment in the Safe Room (Tier 5) or Safe 1 (Equipment Safe) if an SSC is available.

6.15 Equipment Maintenance

To perform maintenance on equipment contained in Safe 1 (Equipment Safe), the equipment MUST be moved to the Key Ceremony Room (Tier 4) by a CA accompanied by an IW and SSC in order to conduct the maintenance.

7 Unplanned Events

Unplanned events (exceptions) during the ceremony are evaluated, documented, and acted upon. It is the CA's sole responsibility to decide on proper actions after consulting with the IW. In either case, an exception is regarded as an incident, and incident handling procedures are enacted.

If the event is severe enough to abort the ceremony and the ceremony cannot be restarted at the KMF within the critical time frame, the CA MUST report it to RKOS, which in turn MUST report it to the RZ KSK Operator Policy Management Authority (PMA).

Examples of unplanned events that might occur during a ceremony include:

- Hardware failures
- Software failures
- CO credentials failure
- Recovery Key Share failure
- Safe failure
- Safe deposit box failure
- General facility failure

8 Key Management Facility Tiers

Tiers 1 - 3

Tiers 1 - 3 consist of the facility areas between the outside environment and the Key Ceremony Room.

Tier 4

Tier 4 consists of the Key Ceremony Room and is subject to dual occupancy (section 4.6).

Tier 5

Tier 5 consists of the Safe Room (a cage only accessible from the Key Ceremony Room) and is subject to dual occupancy (section 4.6).

Tier 6

Tier 6 consists of Safe 1 (Equipment Safe) and Safe 2 (Credentials Safe).

Tier 7

Tier 7 consists of the HSM stored in Safe 1 (Equipment Safe) and the safe deposit boxes mounted in Safe 2 (Credentials Safe).

9 Tier Access Matrix

The following table lists which roles have access to each facility tier.

Role	Tiers 1 - 3	Tier 4	Tier 5	Tier 6	Tier 7
CA	Yes	Yes, with IW	Yes, with IW	No	No
IW	Yes	Yes, with CA/SA	Yes, with CA	No	No
SSC	No	No	No	Yes	No
CO	No	No	No	No	Yes
RKSH	No	No	No	No	No
SA	Yes	Yes, with IW	No	No	No

10 Number of People Summary

The following table specifies how many people are required per role per KMF and in total for all KMFs, the minimum and maximum amount of people per role, and whether a role is shareable between KMFs (i.e., if someone serving as X for one KMF may also serve as X for another KMF).

Role	Per KMF	Minimum Total	Maximum Total	Shareable?
CA	2	2 (4 preferred)	None	Yes
IW	2	2 (4 preferred)	None	Yes
SSC1	2	4	4	No
SSC2	2	4	4	No
CO	7	14	14	No
RKSH	None	7	7	Yes
SA	2	2 (4 preferred)	None	Yes

11 Number of People per Ceremony

The following table lists the minimum number of people required per role for each ceremony type.

Ceremony Type	CA	IW	SSC1	SSC2	CO	RKSH	SA
Primary HSM Initialization	1	2	1	1	7	7	1
Secondary HSM Initialization	1	2	1	1	7	0-5	1
HSM Introduction	1	2	1	1	3-5*	0-2*	1
HSM Decommission	1	2	1	1	3	0	1
Key Generation	1	2	1	1	3-5*	0-2*	1
Key Signing	1	2	1	1	3	0	1
Private Key Removal	1	2	1	1	3	0	1
SSC1 Enrollment	1	1	1	0	0	0	0
SSC2 Enrollment	1	1	0	1	0	0	0
SSC1 Rotation	1	1	2	0	0	0	0
SSC2 Rotation	1	1	0	2	0	0	0
SSC1 Recovery	1	1	1	0	0	0	0
SSC2 Recovery	1	1	0	1	0	0	0
CO Enrollment	1	1	0	1	7	0	0
CO Rotation	1	1	0	1	2	0	0
CO Recovery	1	1	0	1	1	0	0
CO Tenant Key Disclosure	1	1	0	1	1	0	0
Lock Programming	1	1	0	0	0	0	0
RKSH Rotation	1	1	0	0	0	2	0
SMK or Domain Key Recovery	1	2	1	1	3	5	1
RKSH Recovery	1	2	1	1	3	7	1
Media Deposit	1	1	1	0	0	0	0
Media Extract	1	1	1	0	0	0	0
HSM Acceptance Test	1	1	1	0	0	0	0
Equipment Maintenance	1	1	1	0	0	0	0

*For Thales Luna HSMs, these ceremonies require at least 3 COs, and 2 more TCRs of either CO or RKSH type

*For Keyper HSMs, these ceremonies require at least 3 COs and no additional TCRs

Appendix A: Acronyms

AAK	Adapter Authorization Key
ACS	Access Control System
CA	Ceremony Administrator
CO	Crypto Officer
DNSKEY	Domain Name System Key
DNSSEC	Domain Name System Security Extensions
DR	Disaster Recovery
EW	External Witness
HSM	Hardware Security Module
HVAC	Heating, Ventilation, and Air Conditioning
ICANN	Internet Corporation for Assigned Names and Numbers
IDS	Intrusion Detection System
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 Holder
RRset	Resource Record Set
RRSIG	Resource Record Signature
RZ	Root Zone
SA	System Administrator
SKR	Signed Key Response
SMK	Storage Master Key
SSC	Safe Security Controller
SW	Staff Witness
TCR	Trusted Community Representative
ZSK	Zone Signing Key

Appendix B: Change Log

Revision 3 - 04 October 2018

- Section 1: Added an introductory paragraph.
- Section 2: Added an Objective and Scope section.
- Section 3: Revised text for all roles to improve consistency and to clarify the responsibilities for each role.
- Section 5.2.3: Removed because it was redundant with 5.2.2 #6
- Section 11: Moved the SA column so the table would have roles in the same order as previous tables.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Appendix A: Updated to reflect only the acronyms present in the document.
- Sections 3.8 and 3.9: Defined a TCR as someone from the technical Internet Community, not specifically DNS Community.
- Section 4.5: Defined a courier as someone with a Trusted Role.
- Section 5.2.1: Updated to reflect accurate HSM initialization procedures.
- Section 5.2.2: Updated to reflect RKSH storage method.
- Section 6.1 and 6.2: Updated to reflect current practices for SSCs.
- Section 11: Updated to require 5 RKSH and 1 SA for RKSH Recovery.

Revision 3.2 - 07 April 2020

- Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5.5: Updated ceremony scheduling window.

Revision 3.3 - 04 November 2020

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Overall: Uniformly specified “common key” as “guard key”.
- Overall: Uniformly specified “unique key” as “tenant key”.
- Overall: Uniformly specified “Tier 4” as “Tier 4 (Key Ceremony Room)”
- Overall: Uniformly specified “Tier 5” as “Tier 5 (Safe Room)”
- Overall: Substituted references to safe deposit box logbook for safe audit log.
- Overall: Substituted references to site for KMF (Key Management Facility).
- Section 1: Defined Key Management Facility (KMF).
- Section 3.2: Defined minimum number of Ceremony Administrators per KMF.
- Section 3.4: Defined minimum number of System Administrators per KMF.
- Section 3.5: Defined minimum number of Internal Witness per KMF.
- Section 4.5: Clarified key distribution process.
- Section 5.5.1: Updated and added scenarios defining pre-publication, post-publication, rollover, and revocation of Trust Anchors.
- Section 5.5.2: Added SKR handling procedures in disaster recovery scenarios.
- Section 6.1: Clarified scenario explanation for SSC enrollment.

- Section 6.2: Specified steps which can be performed by the remaining SSC.
- Section 6.3: Clarified scenario explanation for SSC combination recovery.
- Section 6.4: Clarified scenario explanation for CO enrollment.
- Section 6.5: Clarified scenario explanation and steps for SSC replacement.
- Section 6.6: Clarified scenario title and explanation for CO tenant key unavailability recovery to suit multiple situations.
- Section 6.7: Added tamper-evident bag MAY be replaced during RKSH replacement.
- Section 6.9: Clarified scenario explanation for media deposit.
- Section 6.10: Clarified scenario explanation for media extraction.
- Section 6.11: Clarified scenario explanation for equipment acceptance testing.
- Section 6.12: Clarified scenario explanation for equipment maintenance.
- Section 8: Clarified definition of tier 5.
- Section 9: Clarified Tier Access Matrix for CO role in tier 7.
- Section 10: Updated table and included personnel limits.
- Section 11: Update personnel required and added HSM Introduction and SMK Recovery scenarios.

Revision 3.4 - 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
- Section 6.8: Defined scenario and actions for an unavailable RKSH or RKSH credential

Revision 3.5 - 19 October 2022

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 6.2: Removed step 5 to attempt the old combination as it is unnecessary.
- Section 6.5: Updated to reflect the possibility of scheduling a lock replacement instead of having to do it immediately.
- Section 6.7: Created scenario for a CO tenant key recovery disclosure ceremony.
- Section 6.8: Created scenario for a safe deposit box lock programming ceremony.
- Section 11: Table updated with newly added administrative ceremony types.

Revision 3.6 - 12 October 2023

- Annual review: Update version information and dates.

Revision 3.7 - 15 March 2024

- Update version information and dates
- Section 3.9: Revised Recovery Key Share Holder section to cover Thales Luna hardware and its keys and credentials
- Section 5: Revised Key Management Ceremonies to cover the credential distribution design for the Thales Luna and Keyper hardware simultaneously
- Section 5.2: Revised HSM Initialization section and subsections to cover the credential distribution design for the Thales Luna and Keyper hardware simultaneously
- Section 5.4: Revised Key Generation section and subsections to cover the credential distribution design for the Thales Luna and Keyper hardware simultaneously

- Section 6.9: Revised RKSH Replacement section to cover the credential distribution design for the Thales Luna and Keyper hardware simultaneously
- Section 6.11: Revised Issuing New Recovery Key Shares section to cover the credential distribution design for the Thales Luna and Keyper hardware simultaneously
- Section 6.12: Corrected erroneous reference to section 6.10 with corrected reference to section 6.13
- Section 6.14: Revised Equipment Acceptance Testing section to cover additional features of the Thales Luna hardware
- Section 11: Revised Number of People Per Ceremony table to cover scenarios with both Keyper and Thales Luna hardware and credentials