Root Zone KSK Operator Key Management Policy

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

All cryptographic operations involving the RZ KSK are conducted within physically protected environments 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 policy is to 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 objectives of this policy are:

- Cryptographic keys are securely generated.
- Private components of the keys remain secret, including during key distribution, and their integrity and authenticity is retained.
- Public components of the keys are securely distributed.
- Cryptographic keys are available when they are needed and are only used for their intended purpose.
- All instances of the private keys are properly destroyed at the end of their designated lifetime.
- Access to cryptographic hardware is limited to authorized individuals.

The critical cryptographic keys are the RZ Key Signing Key, Domain Key, Crypto Officer (CO) Key, and Storage Master Key (SMK).

3 Roles and Responsibilities

This policy is applicable to all staff involved in the RZ KSK Operator function. The staff involved in the RZ KSK Operator function MUST comply with the information security policies found in this and other related information security documents. Staff who deliberately violate this and other information security policy statements will be subject to disciplinary action which MAY ultimately include termination.

4 Security Requirements

4.1 Availability

The organization MUST be able to accommodate a Key Ceremony (with operational key material) with at least 30 days' notice.

4.2 Integrity and Confidentiality

The integrity and confidentiality of the private key MUST to the utmost possible extent be maintained. Undetected theft, tampering, or unauthorized use of the private component of the RZ KSK is completely unacceptable.

5 Security Controls

This section defines the security controls REQUIRED to mitigate the identified vulnerabilities to an acceptable level of risk.

5.1 Security Management

Key management is the secure administration and distribution of cryptographic keys throughout the entire key lifecycle. Keys are generated, distributed, backed up, used, possibly recovered, and eventually terminated. The states for the management of any RZ KSK lifecycle are defined in Figure 1.

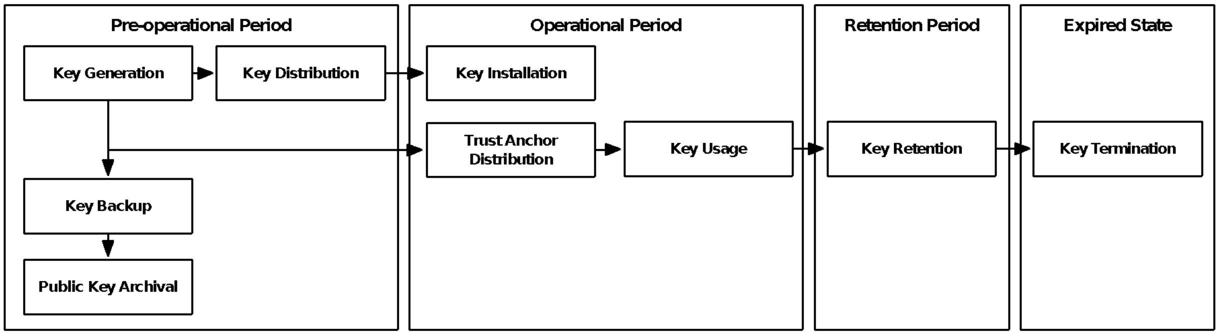

Figure 1: Key lifecycle for KSK

To support this process, this key management policy MUST be maintained and periodically reviewed (at least annually) by the RZ KSK Operator Policy Management Authority (PMA). Reviews MUST be documented in the change log of this document, and the following roles and responsibilities MUST be assigned:

- RZ KSK PMA: The PMA is a committee responsible for overseeing the lifecycle of the RZ KSK Operator function. Refer to the PMA charter for a complete list of responsibilities and members.
- RZ KSK Operations Security (RKOS): RKOS is a security support and coordination role responsible for following up on incident reporting, providing assistance to the external auditors, conducting internal audits, initiating security awareness activities, providing security

training, providing security expertise guidance to the PMA, overlooking the lifecycle management of the RZ KSK Operator function, and maintaining all related documentation.

Any changes or deviations from this policy MUST be approved by the PMA and documented to maintain an audit trail.

5.2 Key Management Environment

Any Domain Name System Security Extensions (DNSSEC) operational activity and any activity related to the lifecycle of the RZ KSK MUST occur within the RZ KSK Operator-controlled secure Key Management Facilities. Application Keys which are within their Operational Period, and Domain keys and SMKs used to protect Application Keys within their Operational Period MUST NOT be used outside of the Key Management Facility.

Each facility MUST have redundant sets of working equipment, and the equipment MUST be maintained.

All components required to activate the Hardware Security Modules (HSMs) and perform any key operations MUST be stored within each Key Management Facility. Emergency recovery procedures to assemble a complete working set of equipment MUST be documented in the “Disaster Recovery Plan”.

5.3 Cryptographic Environment

All cryptographic functions involving the private component of the RZ KSK MUST be performed within a Federal Information Processing Standard (FIPS) 140-2 validated HSM at level 4 overall (current or historical), or an HSM currently under review for or validated to FIPS 140-3 level 3 overall.

The private component of the RZ KSK MUST only be exported from the HSM for purposes of distribution and backup in accordance with section 5.5, 5.6, and 5.8 in this policy.

Activation of any HSM containing Application Keys within their Operational Period, or Domain, CO, and SMK Keys used to protect Application Keys within their Operational Period, MUST require three (3) of seven (7) Crypto Officers selected from organizationally separate parties not affiliated with PTI, ICANN, or Verisign.

5.4 Key Generation

All KSK key pairs MUST be generated at pre-planned Key Generation Ceremonies. Roles, responsibilities, and provisions for the Key Generation Ceremony MUST be described in detail in the “Key Management Procedures” and MUST comply with this policy.

Selected algorithms and key lengths MUST be both resource efficient and of sufficient strength to prevent others from determining the key private component using cryptanalysis during the period of expected utilization of such key pairs, which is currently estimated to be five years.

The current RZ KSK pair MUST therefore be an RSA key pair with a modulus size of 2048 bits. Key generation and selection of key parameters for the RZ KSK or any other key for which the confidentiality of the RZ KSK depends MUST be in compliance with FIPS 140-2 or FIPS 140-3.

5.5 Key Distribution

Keys generated using Keyper HSMs MUST be distributed by exporting the Application Key(s), symmetrically encrypted with the SMK, onto two smartcards destined for each Key Management Facility, including the facility used for key generation (for backup purposes). The algorithm used for encrypting the Application Key(s) MUST comply with "NSA Suite B Cryptography". The aforementioned smartcards MUST be placed in signed, labeled, and sealed tamper-evident bags at the ceremony before being carried out of the secure facility.

Keys generated using Thales Luna HSMs MUST be distributed by cloning or backing up the Application Key(s), protected by the CO and Domain Keys, onto two Thales Luna Backup HSMs destined for each Key Management Facility, including the facility used for key generation (for backup purposes). The algorithm used for encrypting the Application Key(s) MUST comply with "NSA Suite B Cryptography". The aforementioned Thales Luna Backup HSMs MUST be placed in signed, labeled, and sealed tamper-evident bags at the ceremony before being carried out of the secure facility.

Key material, when physically transported between Key Management Facilities, MUST be couriered by RZ KSK Operator personnel who hold a Trusted Role in the RZ KSK Operator function.

Keys MUST NOT enter their Operational Period (published as Trust Anchors or included in the Domain Name System Key (DNSKEY) Resource Record Set) until key distribution to all active Key Management Facilities has been completed. Key distribution MUST be considered completed after all smartcards or backup HSMs have reached their final destinations and are safely stored within these Key Management Facilities. After key distribution has been completed, a KSK MAY enter its Operational Period.

If the chain of custody for any of the key distribution smartcards or backup HSMs is lost during key distribution, the key(s) stored on these smartcards or backup HSMs MUST be considered compromised and MUST NOT enter an Operational State.

The SMK or Domain Key MUST be generated within an HSM during an HSM Initialization Ceremony. The SMK or Domain Key MUST be exported using a five (5) of seven (7) threshold secret sharing scheme and distributed to organizationally separate parties (Trusted Community Representatives [TCRs]) not affiliated with PTI, ICANN, or Verisign. Specifically, any one person or organization MUST

NOT ever hold the complete SMK or Domain Key currently in use to protect keys within their Operational Period.

For managing the Recovery Key Share Holders (RKSHs), the RKOS function MUST be responsible for:

- Establishing and maintaining the list of RKSHs and their assigned shares
- Organizing and supporting any handovers and recovery of shares
- Conducting a yearly inventory of shares, where each RKSH MUST provide proof of being in possession of the shares at the time of the inventory

The requirements and provisions for the management of RKSHs MUST be described in detail in the "Key Management Procedures" and MUST comply with this policy.

If temporary SMK or Domain Key shares are used for distribution of pre-operational keys, the same requirements apply to the set of those shares as to the smartcards or backup HSMs holding the application keys, but these shares MUST be destroyed before the Application Keys can enter their Operational Period, and their chain of custody MUST be maintained until the time of destruction. During key distribution, the packages containing the temporary SMK or Domain Key shares MUST be split over several persons, so that no one courier can reassemble the key.

5.6 Trust Anchor Distribution

As a KSK enters its Operational Period, the public portion of the RZ KSK MUST be posted on the RZ KSK Operator's repository as a Trust Anchor. The method(s) to validate its integrity MUST be publicly available (out-of-band) as an Internet Engineering Task Force (IETF) Informational RFC.

The mechanisms described to validate the RZ KSK public key(s) MUST establish proof of possession of either the RZ KSK private key or the previous RZ KSK private key.

The RZ KSK public key(s) MUST be exported and distributed in a secure fashion to preclude substitution attacks. The procedures for exporting the keys MUST be documented in the "Key Management Procedures". The current format for publication and the method(s) to validate its integrity is documented in the [RFC 7958] "DNSSEC Trust Anchor Publication for the Root Zone" document.

5.7 Key Installation

Installation of distributed key material MUST be conducted at a Key Installation Ceremony. Roles, responsibilities, and provisions for the Key Installation Ceremony MUST be described in detail in the "Key Management Procedures" and MUST comply with this policy.

5.8 Key Backup

Key backup MUST be conducted at each Key Generation Ceremony by exporting the KSKs (Application Keys), protected by the SMK or Domain Key, onto two smartcards or backups HSMs for each Key Management Facility, including the facility used for key generation as part of the key distribution process. The algorithm used for encrypting the KSKs MUST comply with “NSA Suite B Cryptography”.

The smartcards or backup HSMs containing the Application Keys MUST be placed within signed, sealed, and serial-numbered tamper-evident bags stored within the equipment safe together with the HSM.

5.9 Key Recovery

Key recovery procedures for recovery of Application Keys, Domain Keys, and the SMK MUST be documented in detail in the “Key Management Procedures” document, and cover the following scenarios:

5.9.1 Recovery of Application Keys

- Application Keys to be restored on an HSM that has the SMK or Domain Key installed, using backup smartcards or backup HSMs or another HSM at a site.
- Application Keys and SMK or Domain Keys to be restored on one HSM using another HSM, temporary SMK shares if required, and backup smartcards or backup HSMs.
- Application Keys and SMK or Domain Key to be restored on both HSMs at a site using the RKSH and backup smartcards or backup HSMs.
- SMK or Domain Key to be restored on both HSMs at a site, and roll into new Application Keys (recovery from complete loss of Application Keys).

5.9.2 Recovery of Domain Key (with a 5 of 7 sharing threshold)

- At least two (2) shares, but not more than four (4) shares, are permanently lost.
- More than four (4) shares are permanently lost.

5.9.3 Recovery of SMK (with a 5 of 7 sharing threshold)

- At least two (2) shares, but not more than four (4) shares, are permanently lost.
- More than four (4) shares are permanently lost.

The key recovery procedures MUST also include emergency procedures if the required number of TCRs are unavailable for a Key Ceremony.

5.10 Key Usage

The RZ KSK private key MUST be activated using three (3) of seven (7) CO controlled credentials that MUST be inserted into the HSM, one at a time, while entering the crypto officers' PIN if required. The PIN MUST be set to "11223344" for all smartcards.

The sufficient number (with respect to the m of n requirement) of COs MUST be present for as long as the HSM is activated. The RZ KSK private keys MUST be deactivated upon system shutdown.

For managing the COs, the RKOS function MUST be responsible for:

- Establishing and maintaining the list of COs and their assigned safe deposit box keys
- Organizing and supporting any handovers and recovery of safe deposit box keys

Any RZ KSK private key MUST only be used for signing the root zone's DNSKEY resource record set (RRset) or self-signing using the same padding scheme in order to prove possession of the private key. The Zone Signing Key (ZSK) Operator keys MUST be authenticated using either proof traceable to the last set of keys, or using out-of-band authentication of recognized representatives of the ZSK Operator, attesting to the authenticity of the key set.

Any resource record signature (RRSIG) record generated as a result of a KSK signing operation MUST NOT have a validity period longer than 21 days, and MUST NOT expire more than 180 days in the future.

Disaster recovery procedures may override the standard RRSIG expiration period if reasonable concerns exist regarding the ability to conduct subsequent key signing operations during their allotted window. Additional RRSIG records may be generated further in advance of the standard validity period, which would remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set would not expire more than 180 days in the future. The RZ KSK Operator will withhold RRSIG records generated for future validity periods using methods which reasonably safeguard the confidentiality, integrity, and availability of the RRSIG records utilizing a KMF and an offsite storage facility until they are transmitted to the RZ ZSK Operator. This scenario requires consent between the RZ KSK and RZ ZSK Operators and approval from their respective executive management.

The Operational Period of an RZ KSK MUST end upon its supersession and then enter the retention state. The superseded RZ KSK MUST NOT be reused to sign a resource record while in retention.

5.11 Key Termination

After a superseded KSK has been in retention for 30 days, it MUST enter into the expired state. Any private key in the expired state MUST be destroyed at the next Key Ceremony at each site.

The keys MUST be destroyed in a manner that reasonably ensures there are no residual remains that could lead to key reconstruction. The procedure for key destruction MUST be documented in the “Key Management Procedures” document.

5.12 Key Archival

The RZ KSK private key and the SMK MUST NOT be archived.

5.13 Media Storage

Any media or device containing Application Keys within their Operational Period MUST NOT be handled, stored, or transported outside of the secure facilities at any time in any form.

All other media containing software, application data, audit information, and other information relevant to KSK operations MUST be stored within the facilities or a secure offsite storage facility.

Any media, when not under the constant observation of a Trusted Person, MUST be stored within signed and sealed, serial-numbered, tamper-evident bags.

Appendix A: Acronyms

CO	Crypto Officer
DNSKEY	Domain Name System Key
DNSSEC	Domain Name System Security Extensions
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
KSK	Key Signing Key
NSA	National Security Agency
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
SMK	Storage Master Key
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.

Revision 3.1 - 28 October 2019

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5.3: Removed “Refer to R. Lamb, “Trusted Community Representatives -- Proposed Approach to Root Key Management,” April 2010.”

Revision 3.2 - 07 April 2020

- Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5.10: Updated to reflect scenarios where additional RRSIGs may be generated.

Revision 3.3 - 04 November 2020

- Annual review: Update version information and dates.
- Made minor formatting changes.
- Section 5.4: Removed “FIPS 186-2” because it is referenced in FIPS 140-2, and now reflects the requirements stated in the DPS section 5.2.1 “Cryptographic Module Standards and Controls.”
- Section 5.10: Defined RRSIG storage policy and required management approval level.

Revision 3.4 - 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 3.5 - 19 October 2022

- Annual review: Update version information and dates.
- Made minor editorial, formatting, and style changes.
- Section 5.9: Clarified “key” as “safe deposit box key.”

Revision 3.6 - 12 October 2023

- Annual review: Update version information and dates.

Revision 3.7 - 15 March 2024

- Update version information and dates
- Overall: Performed updates to cover the use of Keyper and Thales Luna HSMs simultaneously
- Section 2: Revised critical cryptographic keys to include Domain and CO Keys used by Thales Luna HSMs

- Section 5.2: Revised Key management environment to include keys used by Thales Luna HSMs
- Section 5.3: Cryptographic environment expanded to cover the Thales Luna HSM FIPS certification level along with its respective keys
- Section 5.4: Included FIPS 140-3, the updated standard replacing FIPS 140-2
- Section 5.5: Revised key distribution section to cover Thales Luna hardware and its keys and credentials
- Section 5.8: Revised key backup section to cover Thales Luna hardware and its keys and credentials
- Section 5.9: Revised key recovery section and subsections to cover Thales Luna hardware and its keys and credentials
- Section 5.10: Revised key usage section to cover Thales Luna hardware and its keys and credentials