Verisign DNSSEC Practice Statement for the Root Zone ZSK Operator

Version: 2.2

Effective Date: July 18, 2024

Abstract

This document is the DNSSEC Practice Statement (DPS) for the Root Zone (RZ) Zone Signing Key (ZSK) operator. It states the practices and provisions that are used to provide Root Zone signing and zone distribution functions, such as: issuing, managing, changing and distributing Domain Name System (DNS) ZSKs, for the Root Zone service.

Table of Contents

1. INTRODUCTION

This document is the Verisign DPS for the RZ ZSK operator. It states the practices and provisions that Verisign employs in providing Root Zone signing and zone distribution services that include, but are not limited to, issuing, managing, changing and distributing DNS ZSKs, for the Root Zone service.

1.1 Overview

The Domain Name System Security Extensions (DNSSEC) is a set of Internet Engineering Task Force (IETF) specifications for adding origin authentication, data integrity, and authenticated denial of existence to theDNS. DNSSEC provides a way for software to validate that DNS data has not been modified during Internet transit. This is one by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating at the Root Zone.

The DNS was not originally designed with strong security mechanisms to provide origin authentication, data integrity and authenticated denial of existence to the DNS. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system. DNSSEC addresses these vulnerabilities by adding data origin authentication, data integrity and authenticated denial of existence capabilities to the DNS.

This DPS is specifically applicable to the Root Zone Maintainer and RZ ZSK operator. Verisign performs these roles by virtue of its Root Zone Maintainer Agreement with the Internet Corporation for Assigned Names and Numbers (ICANN). More generally, this document will provide the governing policies and provisions as it relates to the management, security and technical specifications of DNSSEC operation at the Root. This document will be under the control and management of Verisign. Information in this document and subsequent documents will be made public as required.

The DPS is only one of a set of documents relevant to Verisign's management of the Root Zone's ZSK. Other documents include: ancillary confidential security and operational documents that supplement the DPS by providing more detailed requirements, such as:

> The Verisign Physical Security Policy – Describes physical and personnel security requirements;
> Verisign information security documentation - Describes information security requirmements;
> The Verisign Cryptographic Key Management Guide – Describes cryptographic key management security; and
> The Verisign Key Ceremony Reference Guide - Describes the procedures used to manage cryptographic keys.

In many instances, the DPS refers to one or more of the above ancillary documents for specific, detailed practices. These ancillary documents are considered Verisign sensitive information and will not be publicly disclosed.

1.2 Document Name and Identification

Document title:

> DNSSEC Practice Statement for the Root Zone ZSK Operator

Version:

2.2

Date:

TBD

1.3 Community and Applicability

1.3.1 Root Zone Manager

Public Technical Identifiers (PTI) performs the management of the DNS Root Zone. This role includes accepting change requests to the contents of the Root Zone from the Top Level Domain (TLD) operators and validating those requests. After validation occurs, implementation is performed by the Root Zone Maintainer.

PTI is an affiliate of the Internet Corporation for Assigned Names and Numbers (ICANN), and performs these functions under an "IANA Naming Functions" contract from ICANN using the facilities, property and staff of ICANN under a service agreement.

1.3.2 Root Zone Maintainer

Verisign is acting as the Root Zone Maintainer. The Root Zone Maintainer performs the function of receiving change requests to the Root Zone from the Root Zone Manager, implementing the changes, generating a new Root Zone file and distributing it to the Root Server operators.

1.3.3 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. The Root Server operators are not involved in the making of any policies or modification of data.

1.3.4 Root Zone Key Signing Key Operator

PTI performs the Root Zone Key Signing Key (RZ KSK) operator function of generating the Root Zone's Key Signing Key (KSK) and signing the Root Keyset, including the Root Zone Zone Signing Key (RZ ZSK), using the KSK. The Root Zone 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.

The RZ KSK operator is responsible for:

1. Generating and protecting the private component of the RZ KSK.
2. Securely importing public key components from the RZ ZSK operator.
3. Authenticating and validating the public RZ ZSK keyset.
4. Securely signing the RZ ZSK keyset.
5. Securely transmitting the signed RZ ZSK key set to the RZ ZSK operator.
6. Securely exporting the RZ KSK public key components.
7. Issuing an emergency key roll-obrt within a reasonable amount of time if any private key component associated with the zone is lost or suspected to be compromised.

1.3.5 Root Zone 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 ZSK operator is responsible for:

1. Generating and protecting the private component of the RZ ZSK.
2. Securely exporting and transmitting the public RZ ZSK component to the RZ KSK operator.
3. Securely importing the signed RZ ZSK keyset from the RZ KSK operator.
4. Signing the Root Zone's resource records (optionally omitting the DNSKEY resource record).
5. Issue emergency key rollover within a reasonable amount of time if any private key associated with the zone is lost or suspected to be compromised.

1.3.6 Child Zone Manager

The child zone (TLD) manager is a trustee for the delegated domain, and as such responsible for providing registry services and operating subordinate DNS servers. If a child zone is signed using DNSSEC, the child zone manager is also responsible for:

1. Generating the keys associated with its zone using a trustworthy method.
2. Registering and maintaining the shorthand representations of its KSK (Delegation Signer [DS] Resource Record) in the parent zone to establish the chain of trust.
3. Taking reasonable precautions to prevent any loss, disclosure or unauthorized use of the keys associated with its zone.
4. Issuing emergency key rollover within reasonable time if any private key associated with its zone is lost or suspected to be compromised.

1.3.7 Relying Party

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

The relying party must properly configure and update the Trust Anchor as appropriate. The automated method described in RFC 5011 [RFC5011] may be used.

Relying parties must also stay informed of any critical changes in the Root Zone operation as notified by ICANN in accordance with RZKSK operator's DPS section 2.1. [RZKSKDPS]

1.3.8 Applicability

This DPS is only applicable to the Root Zone, and more specifically the RZ ZSK operator. Each link in the chain of trust may have entirely different requirements that can affect the end entity, and is not governed by this DPS.

Entities must evaluate their own environments and its associated threats and vulnerabilities to determine the level of risk they are willing to accept.

1.4 Specification Administration

This DPS will be periodically reviewed and updated, as appropriate by the Verisign DNSSEC Policy Management Authority (PMA). The PMA is responsible for the management of the DPS and should be considered as the point of contact for all matters related to the DPS. The PMA notifies and seeks the review and authorization from ICANN prior to taking action and/or modification of the DPS.

1.4.1 Specification Administration Organization

VeriSign Inc
12061 Bluemont Way
Reston, VA 20190
USA

1.4.2 Contact Information

The DNSSEC Practices Manager
Verisign DNSSEC Policy Management Authority
c/o VeriSign, Inc
12061 Bluemont Way
Reston, VA 20190
USA
+1 (703) 948-3200 (voice)
+1 (703) 421-4873 (fax)
dnspractices@verisign.com

1.4.3 Specification Change Procedures

Amendments to this DPS are made by the Verisign DNSSEC Policy Management Authority (PMA). Amendments will either be in the form of a document containing an amended form of the DPS or an update. Amended versions or updates will be linked to the Practices Updates and Notices section of the Verisign Repository located at: https://www.verisign.com/en_US/repository/index.xhtml. (See section 2 for a more detailed explanation of Repositories.) Updates supersede any designated or conflicting provisions of the referenced version of the DPS.

The PMA reserves the right to amend the DPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material is within the PMA's sole discretion. Proposed amendments to the DPS will appear in the Practices Updates and Notices section of the Verisign Repository, which is located at: https://www.verisign.com/en_US/repository/index.xhtml. The PMA solicits proposed amendments to the DPS from the community. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA will provide public notice of such amendment in accordance with this section. Notwithstanding anything in the DPS to the contrary, if the PMA believes that material amendments to the DPS are necessary immediately to stop or prevent a breach of the security of any portion of it, the PMA is entitled to make such amendments by publication in the Verisign Repository. Such amendments will be effective immediately upon publication.

2. PUBLICATION AND REPOSITORIES

2.1 Repositories

Verisign, as the ZSK operator, publishes the DPS in the Verisign repository section of Verisign's web site at https://www.verisign.com/en_US/repository/index.xhtml. Public access to this repository will include the option of using an HTTPS-authenticated channel.

2.2 Publication of Key Signing Keys

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

2.3 Access Controls on Repositories

Information published in the repository portion of the Verisign web site is publicly-accessible information. Read only access to such information is unrestricted. Verisign has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. OPERATIONAL REQUIREMENTS

3.1 Meaning of Domain Names

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.2 Activation of DNSSEC for Child Zone

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.3 Identification and Authentication of Child Zone Manager

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.4 Registration of Delegation Signer (DS) Records

Verisign, as the Root Zone Maintainer, applies changes to the root zone file based on requests from the Root Zone Manager.

3.5 Method to prove possession of private key

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.6 Removal of DS Resource Records

3.6.1 Who Can Request Removal

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.6.2 Procedure for Removal Request

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

3.6.3 Emergency Removal Request

Refer to the RZ KSK operator's DPS for details [RZKSKDPS].

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1 Physical Controls

As the RZ ZSK operator, Verisign has implemented the Verisign Physical Security Policy, which supports the physical security requirements of this DPS. Compliance with these policies is included in Verisign's independent audit requirements described in section 7. Verisign Physical Security Policy contains sensitive security information and will not be publicly disclosed. An overview of the requirements is described below.

4.1.1 Site Location and Construction

Verisign DNSSEC operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt. Verisign also maintains disaster recovery facilities for its DNSSEC operations. Verisign's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of Verisign's primary facility.

4.1.2 Physical Access

Verisign DNSSEC systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive DNSSEC operational activity and any activity related to the lifecycle of the RZ ZSK occur within very restrictive physical tiers.

Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of multi-factor authentication including biometrics. Unescorted personnel, including visitors or employees without specific authorization, are not allowed into such secured areas. The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of Hardware Security Modules (HSMs) and keying material.

Areas used to create and store cryptographic material enforce dual control, each through the use of multi-factor authentication including biometrics. Online HSMs are protected through the use of locked cabinets. Offline HSMs are protected through the use of tamper-evident bags, locked safes and containers. Access to HSMs and keying material is restricted in accordance with Verisign's segregation of duties requirements. The opening and closing of cabinets, safes, or containers in these tiers is logged for audit purposes.

4.1.3 Power and Air Conditioning

Verisign's secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and heating/ventilation/air conditioning systems to control temperature and relative humidity.

4.1.4 Water Exposures

Verisign has taken reasonable measures to minimize the impact of water exposure to Verisign systems.

4.1.5 Fire Prevention and Protection

Verisign has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Verisign's fire prevention and protection measures have been designed to comply with local fire safety regulations.

4.1.6 Media Storage

All media containing production software data, as well as audit, archive, or backup information are stored within Verisign facilities or in a secure off-site storage facility with appropriate physical andlogical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water,fire, and electromagnetic).

4.1.7 Waste Disposal

Sensitive documents are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance or Verisign information security requirements prior to disposal.

4.1.8 Off-site Backup

Verisign performs routine backups of critical system data, audit log data, and other sensitive information. Off-site backup media are stored in a physically secure manner using a bonded third party storage facility and/or Verisign's disaster recovery facility(ies).

4.2 Procedural Controls

4.2.1 Trusted Roles

Trusted Persons include all individuals that have access to or control cryptographic operations that may materially affect:

generation and protection of the private component of the RZ ZSK,
secure export or import of any public components, and
generation and of signing zone file data.

Trusted Persons include, but are not limited to:

Naming Provisioning and Resolution Operations personnel,
Cryptographic Business Operations personnel,
security personnel,
system administration personnel,
designated engineering personnel, and
executives that are designated to manage infrastructural trustworthiness.

Verisign considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in section 4.3.2 of this DPS.

4.2.2 Number of Persons Required Per Task

Verisign has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The most sensitive tasks, such as access to and management of cryptographic hardware (i.e., HSMs) and associated key material require multiple Trusted Persons. These internal control procedures are designed to ensure that at a minimum, two Trusted Persons are required to have either physical or logical access to the device.

Access to cryptographic hardware is strictly controlled by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once an HSM is activated with operational keys, further access controls are invoked to maintain split control over physical access to the device. Persons with physical access to HSMs do not hold "Secret Shares" and vice versa.

Other manual operations such as the signing of zone file data, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated process.

4.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is in person, including a check of well-recognized forms of government-issued identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in DPS section 4.3. Verisign ensures that personnel have achieved Trusted Persons status and departmental approval has been given before suchpersonnel are:

issued access devices and granted access to the required facilities, or
issued electronic credentials to access and perform specific functions on applicable Verisign Information Technology (IT) systems.

4.2.4 Tasks Requiring Separation of Duties

Tasks requiring separation of duties include but are not limited to the generation, management, or destruction of Root Zone DNSSEC key material.

Personnel holding a role in the multi-party access to the RZ KSK do not hold a role in the multi-party access to the RZ ZSK, or vice versa. Designated audit personnel may not participate in the multi-person control for the RZ ZSK or KSK.

4.3 Personnel Controls

4.3.1 Qualifications, Experience, and Clearance Requirements

Verisign requires that personnel seeking to become Trusted Persons undergo an investigation of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as verification of any government clearances necessary to perform operations under government contracts.

4.3.2 Background Check Procedures

All personnel with access to any cryptographic component used with the Root Zone signing process are required to pass a Verisign background check extending back at least three years.

Prior to commencement of employment as a Trusted Person, Verisign conducts background checks which include the following:

confirmation of previous employment,
check of professional references,
confirmation of the highest or most relevant educational degree obtained,
check of credit/financial records to the extent allowed by national laws for the individual's country of residence,
search of criminal records (local, state or provincial, and national),
search of driver's license records, and
search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, Verisign will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for a Trusted Persons role or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- misrepresentations made by the candidate or Trusted Person,
- highly unfavorable or unreliable professional references,
- indications of a lack of financial responsibility, or
- certain criminal convictions.

Reports containing such information are evaluated by Verisign human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check.

Such actions may include measures up to and including the cancellation of offers of employment made to candidates for a Trusted Person's role or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

4.3.3 Training Requirements

Verisign provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. Verisign periodically reviews and enhances its training programs as necessary.

Verisign's training programs may include the following as relevant:

basic DNS/DNSSEC concepts,
job responsibilities,
use and operation of deployed hardware and software,
security and operational policies and procedures,

incident and compromise reporting and handling,
disaster recovery and business continuity procedures.

4.3.4 Retraining Frequency and Requirements

Verisign provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

4.3.5 Job Rotation Frequency and Sequence

Positions are rotated and replaced as needed.

4.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions with respect to this DPS and/or other violations of Verisign policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

4.3.7 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants may be used for Trusted Persons roles. Any such contractor or consultant

is held to the same functional and security criteria that apply to a Verisign employee in a comparable position. Independent contractors and consultants who have not completed or passed the background check procedures specified in DPS section 4.3.2 are permitted access to Verisign's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

4.3.8 Documentation Supplied to Personnel

Verisign provides its personnel the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

4.4 Audit Logging Procedures

4.4.1 Types of Events Recorded

Verisign manually or automatically logs the following significant events:

RZ ZSK key life cycle management events, including:

key generation, backup, storage, recovery, archival, and destruction;
exporting of public key components, and
cryptographic device life cycle management events.

RZ ZSK signing and management events, including:

key activation,
receipt and validation of signed public key material (from the KSK operator),
successful or unsuccessful signing requests, and
key rollover events.

RZ ZSK security-related events, including:

successful and unsuccessful system access attempts,
secure cryptographic actions performed by Trusted Persons,
security sensitive files or records read, written or deleted,
changes to a user's security profile,
system crashes, hardware failures and other anomalies,
firewall and router activity,
facility visitor entry/exit,
system changes and maintenance/system updates, and
incident response handling.

Log entries include the following elements:

date and time of the event,
identity of the entity generating the logged event,
serial or sequence number of entry, for automatic journal entries,
type of event, and
other events as appropriate.

All types of audit log information will contain correct time and date information.

4.4.2 Frequency of Processing Log

Audit logs are examined at least annually for significant security and operational events. In addition, Verisign reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within the Verisign zone signing systems. Audit log processing captures audit log details and documentation for all significant events in an audit log summary. Audit log reviews include an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

4.4.3 Retention Period for Audit Log

All audit log data collected in terms of section 4.4.1 is retained on-site for at least one year after creation and is thereafter archived for at least 10 years.

The media holding the audit log data and the applications required to process the information will be maintained to ensure that the archive data can be accessed for the time period set forth in this DPS.

4.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering. Only authorized Trusted Persons are able to obtain direct access to the audit information.

4.4.5 Audit Log Backup Procedures

Verisign incrementally backs up electronic archives of its RZ ZSK information on a daily basis and performs full backups on a weekly. Copies of paper-based records will be maintained in an secure facility.

4.4.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated or paper based audit logs are captured by Verisign personnel.

Electronic information is incrementally backed up and copies of paper-based records are made as new records are entered in thearchive. These backups are maintained in an off-site secure facility.

4.4.7 Notification to Event-Causing Subject

Where an event is logged by an audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.4.8 Vulnerability Assessments

System security scans are performed on at least a monthly basis to monitor for system vulnerabilities. Patches are applied, as necessary, in accordance with Verisign's Information Security Policy.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and Compromise Handling Procedures

In the event that a potential or actual compromise of any system or application is detected, Verisign will perform an investigation in order to determine the nature of the incident. If the incident is suspected to have compromised the private component of an active ZSK, the emergency ZSK rollover procedure will be enacted. Verisign will follow its incident handling procedures set forth in Verisign information security requirements. Such procedures require appropriate escalation, incident investigation and incident response. Incidents that have compromised the private component of an active ZSK will be communicated to the Root Zone KSK Operator in a reasonable timeframe and otherwise in compliance with the applicable agreements between the parties.

4.5.2 Corrupted Computing Resources, Software, and/or Data

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Verisign Information Security team is notified and Verisign's incident handling procedures are implemented. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Verisign's key compromise or Business Continuity plan will be implemented.

4.5.3 Entity Private Key Compromise Procedures

4.5.3.1 Key Signing Key Compromise

Verisign will support RZ KSK emergency rollover in the case of RZ KSK compromise while following ICANN's procedural direction, as outlined in RZ KSK operator's DPS [RZKSKDPS].

4.5.3.2 Zone Signing Key Compromise

Procedures are in place for unscheduled rollovers. In addition, plans and procedures are in place for key compromise situations.

Upon suspected or confirmed compromise of the RZ ZSK, the Verisign Incident Response Team (VIRT) implements Verisign's key compromise response procedures. This team, which includes Information Security, Cryptographic Business Operations, Production Services personnel, and other Verisign management

representatives, assesses the situation, develops an appropriate action plan in accordance with Verisign's information security requirements and implements the action plan with approval from Verisign executive management and the PMA.

4.5.4 Business Continuity and IT Disaster Recovery Capabilities

Verisign has implemented a disaster recovery site that is physically and geographically separate from Verisign's principal secure facilities for signing operations. Verisign has developed, implemented and tested business continuity and IT disaster recovery plan to mitigate the effects of natural, man-made, or technological disasters. Verisign plans are regularly tested, validated, and updated so that Verisign systems, services and key business functions can be operational in the event of any incident or disaster. Detailed Business Continuity Plans and Technical Disaster Recovery Plans are in place to address the restoration of information systems services and key business functions.

Verisign has in place a formal Incident Response Team (IRT) which is supported by a formal Corporate Incident Management Team (CIMT) and Business Continuity teams to respond to and manage any incident or disaster that impacts Verisign employees, operations, environments, and facilities. Verisign's IT disaster recovery site has implemented the physical security and operational controls required by Verisign Physical Security Policies, the Verisign Cryptographic Key Management Guide, and the Verisign Key Ceremony Guide, to provide for a secure and sound alternative operational environment. In case of an event that requires temporary or permanent cessation of operations from Verisign's primary facility, the IRT and CIMT will initiate Verisign’s business continuity and IT disaster recovery plan. Because Root Zone signing operations on a validated zone file are performed actively, independently and redundantly in both facilities, manual intervention is not required in order for the following functions to proceed following a recovery event at either primary site:

communication with the public,
ability to export KSRs,
generation of ZSKs,
signing of a zone file, and
distributing of the signed zone file.

Verisign's disaster recovery environment is protected by physical controls comparable to the physical security tiers specified in DPS section 4.1.2. Verisign tests its environment at its primary site to support all functions to include DNSSEC functions. Results of such tests are reviewed and kept for audit and planning purposes. When possible, operations are resumed at Verisign’s primary site as soon as possible following any incident or disaster. Verisign maintains redundant hardware and backups of its infrastructure system software at its IT disaster recovery facility. In addition, private keys are backed up and maintained for disaster recovery purposes in accordance with DPS section 5.2.4.

4.6 Entity Termination

Verisign has implemented a DNSSEC termination plan in the event that the roles and responsibilities of the RZ ZSK operator must transition to other entities. Verisign will co-ordinate with the Root Zone Manager in order to execute the transition in a secure and transparent manner.

The DNSSEC termination plan also includes procedures in the case of Root Zone Manager and/or RZ KSK operator termination.

5. TECHNICAL SECURITY CONTROLS

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

RZ ZSK key pair generation is performed by multiple pre-selected, trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the generated keys.

All ZSK key pairs are generated in pre-planned cryptographic key generation ceremonies in accordance with the requirements of the Cryptographic Key Ceremony Guide and other applicable policies. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes as required in section 4.4.3.

5.1.2 Public Key Delivery

Refer to the Root Zone Key Signing Key Operator's DPS for details [RZKSKDPS].

5.1.3 Public Key Parameters Generation and Quality Checking

For all RSA keys utilized for DNSSEC signing, Verisign shall obtain assurance of the validity of the public and private key as required by FIPS 186-5.

Quality checking will also include validating the size of the public exponent to be both resource-efficient and secure.

5.1.4 Key Usage Purposes

Any RZ ZSK private key will only be used for signing the relevant Root Zone RRsets or self-signing with the same scheme to provide proof of possession of the private key.

Any resulting resource record signature (RRSIG) record will have a validity period that is no longer than 15 days, and will not extend more than 15 days in to the future.

5.2 Private Key protection and Cryptographic Module Engineering Controls

All cryptographic functions involving the private component of the ZSK are performed within an authorized HSM; that is, the private component will not be exported from an authorized HSM except in encrypted form for purposes of key backup.

5.2.1 Cryptographic Module Standards and Controls

For RZ ZSK key pair generation and RZ ZSK private key storage, Verisign uses HSMs that are certified at FIPS 140-2 Level 3 and/or FIPS 140-3 Level 3 or above.

5.2.2 Private Key (M of N) Multi-Person Control

Verisign has implemented technical and procedural mechanisms that require the participation of multiple Trusted Persons to perform sensitive cryptographic operations. Verisign uses "Secret Sharing" to split the

activation data needed to make use of an RZ ZSK private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (M) out of the total number (N) of Secret Shares are created and distributed for a particular HSM is required to activate a RZ ZSK private key stored on the HSM. It should be noted that the number of shares distributed (N) for disaster recovery HSMs may be less than the number distributed for primary HSMs, while the threshold number of required shares (M) remains the same. Secret Shares are protected in accordance with this DPS.

5.2.3 Private Key Escrow

Private components of RZ ZSKs are not escrowed.

5.2.4 Private Key Backup

Verisign creates backup copies of RZ ZSK private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within HSMs and associated key storage devices. HSMs used for private key storage meet the requirements of this DPS. Private keys are copied to backup HSMs in accordance with this DPS. Modules containing on-site backup copies of RZ ZSK private keys are subject to the requirements of this DPS. Modules containing disaster recovery copies of RZ ZSK private keys are subject to the requirements of this DPS.

5.2.5 Private Key Storage on Cryptographic Module

Private keys held on HSMs are stored in encrypted form.

5.2.6 Private Key Archival

RZ ZSK key pairs do not expire, but are retired when superseded. Superseded key pairs will be securely retained within HSMs that meet the requirements of this DPS. These key pairs will not be used after their supersession. Decommisioned HSMs will be zeroized and/or physically destroyed.

5.2.7 Private Key Transfer into or from a Cryptographic Module

Verisign generates RZ ZSK key pairs on the HSMs in which the keys will be used, with replication procedures for copying those same keys onto copies used for live signing. In addition, Verisign makes copies of such key pairs for routine recovery and disaster recovery purposes. Where key pairs are backed up to another HSM, such key pairs are transported between HSMs in encrypted form.

5.2.8 Method of Activating Private Key

RZ ZSK private keys will be activated using a minimum of three Secret Shares.

5.2.9 Method of Deactivating Private Key

RZ ZSK private keys may be deactivated by three shareholder-controlled credentials being inserted into the HSM, one at a time, while entering the shareholders' common personal identification number (PIN).

Alternatively, Verisign RZ ZSK private keys may be deactivated upon system shutdown.

5.2.10 Method of Destroying Private Key

Where required, Verisign destroys the RZ ZSK private keys in a manner that reasonably ensures that there are no residual remains of the keys that could lead to the reconstruction of the keys. Verisign utilizes the zeroization function of its HSMs, if able, and other appropriate means to ensure the complete destruction of RZ ZSK private keys. When performed, private key destruction activities are logged.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

RZ ZSK public keys are backed up and archived.

5.3.2 Key Usage Periods

The operational period of each RZ ZSK ends upon its supersession. The superseded RZ ZSK is never reused.

5.4 Activation data

5.4.1 Activation Data Generation and Installation

Activation data (contained in Secret Shares) used to activate HSMs containing RZ ZSK private keys is generated in accordance with the requirements of DPS section 5.1. The creation and distribution of Secret Shares is logged.

When required, activation data for the RZ ZSK private keys are transmitted from the PIN Entry Device to the HSM.

5.4.2 Activation Data Protection

Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities. Secret Shares for the HSMs that contain the RZ ZSK private keys will be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. Verisign will decommission Secret Shares by overwriting and/or physical destruction after decommissioning the associated HSMs.

5.4.3 Other Aspects of Activation Data

Not applicable

5.5 Computer Security Controls

Verisign ensures that the systems maintaining key software and data files are secured from unauthorized access. In addition, Verisign limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Verisign requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. Verisign requires that passwords be changed on a periodic basis.

5.6 Network Security Controls

Verisign performs all of its online signing functions using networks secured in accordance with the Verisign information security requirements and Physical Security Policies to prevent unauthorized access and other malicious activity. Verisign protects its communications of sensitive information through the use of encryption and digital signatures.

Verisign's production network is logically separated from other components. This separation prevents network access except through defined processes. Verisign uses firewalls to protect the production network from internal and external intrusion and to limit the nature and source of network activities that may access production systems that are related to key signing activities.

5.7 Timestamping

For online systems, a time syncing protocol such as Network Time Protocol (NTP) will be utilized for timestamping. For offline systems, time will be derived through a manual procedure before the performance of a ceremony.

Time derived from the procedure will be used for timestamping of:

electronic and paper based audit log records
DNSSEC signatures expiration and inception times

Asserted times are required to be reasonably accurate.

5.8 Life Cycle Technical Controls

5.8.1 System Development Controls

Applications are developed and implemented by Verisign in accordance with Verisign systems development and change management standards. All Verisign software deployed on production systems can be traced to version control repositories.

5.8.2 Security Management Controls

Verisign has mechanisms and/or policies in place to control the configuration of its systems. Verisign creates a hash of all software packages prior to installing the packages on production systems. This hash may be used to verify the integrity of such software for forensic purposes

5.8.3 Life Cycle Security Controls

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system will be applied after formal testing and approval. The origin of all software and firmware will be securely authenticated by available means.

HSMs, which are critical hardware components of the signer system, will be obtained directly from the manufacturer and transported in tamper-evident bags to their destination in the secure facility. Any hardware will be decommissioned well in time before the specified life time expectancy.

6 ZONE SIGNING

The RZ KSK operator provides the RZ ZSK operator with signed and valid RRsets for the RZ ZSK operator's current keys and the KSKs.

The Root Zone Maintainer includes the keyset into the root zone file, adds the Next Secure (NSEC) resource records and creates signatures for all relevant records. The Root Zone is then distributed to the Root Server operators.

6.1 Key Lengths and Algorithms

Key pairs are required to be of sufficient length to prevent others from determining the key pair's private key using crypto-analysis during the period of expected utilization of such key pairs.

The current RZ ZSK key pair(s) is an RSA key pair, with a modulus size of at least 1024 bits.

6.2 Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC resource records as specified in RFC 4034 [RFC4034].

6.3 Signature Format

The cryptographic hash function used in conjunction with the signing algorithm is required to be sufficiently resistant to preimage attacks during the time of which the signature is valid.

The RZ ZSK signatures will be generated by encrypting SHA-256 hashes using RSA [RFC5702].

6.4 Zone Signing Key Rollover

The RZ ZSK is changed every calendar quarter. RZ ZSK rollovers are carried out automatically by the system. New RZ ZSKs are signed at ceremonies as described in section 6.6.

6.5 Key signing Key Rollover

Refer to the Root Zone Key Signing Key Operator's DPS for details [RZKSKDPS].

6.6 Signature Life-Time and Re-Signing Frequency

The signing practice of the Root Zone is divided into quarterly continuous time cycles of approximately 90 days. Time cycles begins at the following dates each year:

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

For each of these time cycles there is a key ceremony scheduled approximately 60 days, but no later than 33 days before the time cycle commences. At this key ceremony, all of the necessary RZ KSK operations are performed to enable the Root Zone Maintainer to operate and publish the zone independently throughout the period.

To facilitate automatic updates of resolvers' Trust Anchors as described in RFC 5011 [RFC5011], while minimizing the number of keys in the key set, each of the ~90 day time cycle is divided into 10 day slots (9 slots).

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

For each of these slots there is a pre-generated DNSKEY key set which is signed at the key ceremony with at least 15 days validity time to allow for up to 50% overlap. The Root Zone Maintainer is responsible for selecting the current key set and publishing it with the corresponding valid signature.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

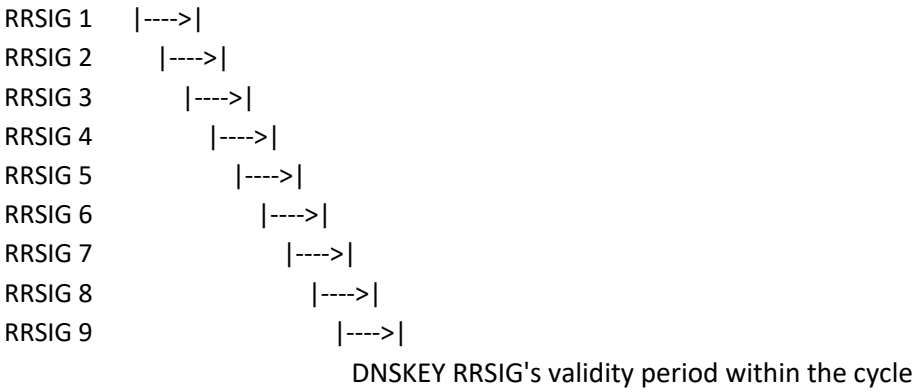

Figure 1

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

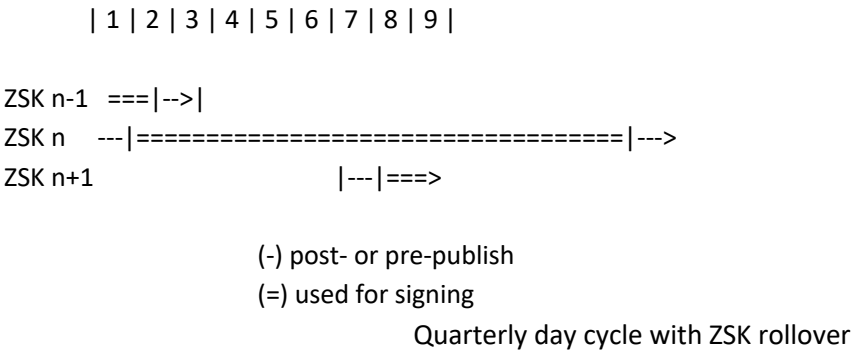

Figure 2

In the event of an RZ ZSK rollover, time slots are used for pre-publish and post-publish in the following order;

Slot 1:

publish ZSK (n) + ZSK (n-1) + KSKs, sign zone with ZSK (n)

Slot 2-8:

publish ZSK (n) + KSKs, sign zone with ZSK (n)

Slot 9:

publish ZSK (n) + ZSK (n+1) + KSKs, sign zone with ZSK (n)

The Root Zone is then published. At each publication the Root Zone Maintainer selects and includes the current DNSKEY RRset and corresponding signature(s), and then signs all other authoritative records within the Root Zone using the current RZ ZSK with a validity period set to at least 13 days.

The Root Zone Maintainer may post-publish a ZSK for more than one slot in extraordinary circumstances, such as when increasing key lengths or changing algorithms. In such circumstances, the details shall be clearly communicated to the parties identified in section 1.3.

6.7 Verification of Zone Signing Key Set

Each key set within the Key Signing Request (KSR) is self-signed with the active key to provide proof of possession of the corresponding private key. The signer system will automatically validate this signature and perform checking of available parameters before accepting the KSR for signing.

The RZ KSK operator will verify the authenticity of the KSR document by performing an out-of-band verification (verbally over the phone, by fax, or any other available method) of the hash of the KSR, before entering the KSR into the signer system. The resulting Signed Key Response (SKR) is transferred back using the same mutually authenticated TLS connection used to receive the KSR from the Root Zone Maintainer.

In the event of an incident which prevents SKR transmission through the standard mechanism, an out-of-band method (such as in person, or via cryptographically signed e-mail) may be used to facilitate the exchange, so long as the identity of the exchanging parties can be verified as authorized representatives of the Root Zone KSK operator and Root Zone Maintainer, respectively.

In case a key rollover requires special attention due to a significant change (e.g. key length, algorithm) and a fallback mechanism is needed, there may be instances when multiple KSRs are generated and submitted to the RZ KSK operator for signing.

6.8 Verification of resource records

The signature verification will be performed using the published RZ Trust Anchor (TA) on the Extractor/Validator system, which holds both the signed data and the unsigned data prior to the zone distribution in order to carry out the verification. Prior to signing, the integrity of the unsigned Root Zone is validated by a different system. The integrity of the non-signed contents will also be performed as part of this validation process.

6.9 Resource Records Time-to-Live

RR Type	**Time-To-Live (TTL)**
DNSKEY	48 hours
DS	24 hours
NSEC	Same as the SOA minimum (24 hours)
RRSIG	Same as the covered RRset (varies)

7 COMPLIANCE AUDIT

An annual independent compliance audit for DNSSEC operations examination is performed for Verisign's data center operations and key management operations supporting Verisign's Root Zone Zone signing services including the RZ ZSK management.

7.1 Frequency of Entity Compliance Audit

Independent audits are conducted at least annually at the sole expense of the audited entity.

7.2 Identity/Qualifications of Auditor

Verisign's compliance audits are performed by a public accounting firm that: Demonstrates proficiency in DNSSEC public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

7.3 Auditor's Relationship to Audited Party

Compliance audits of Verisign's operations are performed by a public accounting firm that is independent of Verisign. Third party auditors do not participate in the multi-person control for the RZ ZSK.

7.4 Topics Covered by Audit

The scope of Verisign's annual compliance audit includes all DNSSEC operations. This includes key environmental controls, key management operations, infrastructure/administrative controls, RZ ZSK and signature life cycle management and practices disclosure.

7.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of Verisign's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by Verisign management. Verisign management is responsible for developing and implementing a corrective action plan. If Verisign determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the RZ ZSK, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, Verisign management will evaluate the significance of such issues and determine the appropriate course of action.

7.6 Communication of results

A copy of Management's Assertion letter can be found at
https://www.verisign.com/en_US/repository/index.xhtml

8. LEGAL MATTERS

8.1 Fees

Not applicable

8.2 Financial Responsibility

Not applicable

8.3 Confidentiality of Business Information

8.3.1 Scope of Confidential Information

The scope of confidential information is set forth in the applicable agreements between the parties.

8.3.2 Information not Within the Scope of Confidential Information

Not applicable.

8.3.3 Responsibility to Protect Confidential Information

Not applicable.

8.4 Privacy of Personal Information

8.4.1 Information Treated as Private

Not applicable.

8.4.2 Information not Deemed Private

Not applicable.

8.4.3 Responsibility to Protect Private Information

Not applicable.

8.4.4 Disclosure Pursuant to Judicial or Administrative Process

Not applicable.

8.5 Limitations of Liability

To the fullest extent permitted by applicable law, in no event shall Verisign or its affiliates, or its or their respective officers, members, directors, employees, service providers, agents, licensors, suppliers, successors and assigns be liable for any direct, indirect, consequential, incidental, special, punitive or exemplary damages whatsoever arising under, related to, or resulting from its performance of its obligations hereunder.

8.6 Term and Termination

8.6.1 Term

The DPS, and any subsequent amended versions, becomes effective upon publication in the Verisign repository.

8.6.2 Termination

This DPS is amended from time to time and will remain in force until it is replaced by a new version.

8.6.3 Dispute Resolution Provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

8.6.4 Governing Law

This DPS shall be governed by the laws of the Commonwealth of Virginia.

9 REFERENCES

9.1 Normative References

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <http://www.rfc-editor.org/info/rfc5011>.

[RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, DOI 10.17487/RFC5702, October 2009, <http://www.rfc-editor.org/info/rfc5702>.

9.2 Informative References

Title: DNSSEC Practice Statement for the Root Zone KSK Operator

Date: October 1, 2016

Author: Root Zone KSK Policy Management Authority

URL: https://www.iana.org/dnssec/dps

Appendix A. Table of acronyms and definitions

A.1. Acronyms

Acronym	Term
AD	**Authenticated Data Flag**
AICPA	American Institute of Certified Public Accountants
BIND	Berkley Internet Name Domain
CBO	Cryptographic Business Operations
CC	Common Criteria
CD	Checking Disabled
DNS	Domain Name System
DNSKEY	Domain Name System Key
DNSSEC	Domain Name System Security Extensions
DO	DNS OK
DPS	DNSSEC Practice Statement
DS	Delegation Signer
EAL	Evaluation Assuance Level (Pursuant to Common Criteria)
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IT	Information Technology
ISO	International Organization for Standardization
KSK	Key Signing Key
KSKO	Key Signing Key Operator

KSR	Key Signing Request
NIST	National Institute of Standards and Technology
NS	Name Server
NSEC	NextSecure
NSEC3	NextSecure3
NTP	Network Time Protocol
PII	Personal Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PTI	Public Technical Identifiers
RFC	Request for Comments
RRSIG	Resource Record Signature
RZ	Root Zone
RZMS	Root Zone Management System
SEP	Security Entry Point
SHA	Secure Hash Algorithm
SKR	Signed-Key Response
SOA	Start of Authority
SP	NIST Special Publication
TLD	Top Level Domain
TSIG	Transaction Signature
TTL	Time-To-Live
VIRT	Verisign Incident Response Team
ZSK	Zone Signing Key
ZSKO	Zone Signing Key Operator

A.2. Definitions

Term	Definition
Chain of Trust	DNS keys, signatures and delegation signer records linked together forming a chain of signed data.
Child Zone	A boundary of responsibility for a domain that exists one level higher than the referenced zone.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other modification, unauthorized use, or other compromise of the security of such private key.
Compliance Audit	A periodic audit that Verisign undergoes to determine its conformance with standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private.
Cryptographic Key Generation Ceremony	A procedure whereby a key pair is generated within a cryptographic module.
Delegation Signer (DS)	A resource record indicating that the delegated zone is digitally signed. It also assures that the parent zone recognizes the indicated key for the delegated zone.
DNSKEY	A resource record that stores the public version of a KSK or ZSK.
Intellectual Property Rights (IPR)	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Island of Security	A signed zone that does not have a chain of trust from the parent zone.
Key Signing Key (KSK)	A key that signs the DNSKEY RRset.

Key Signing Request (KSR)	A file that lists all of the Zone Signing Keys set to be signed by the Key Signing Key for a particular time period, including all the necessary signature inception and expiration dates.
Management Review	Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Offline HSM	An HSM that is maintained offline for security reasons in order to protect it from possible attacks by intruders by way of the network. This HSM does not directly sign the zone file.
Online HSM	An HSM that signs the zone file using the Zone Signing Key and is maintained online so as to provide continuous signing services.
Parent Zone	A boundary of responsibility for a domain with at least one subdomain.
Policy Management Authority (PMA)	The organization within Verisign responsible for promulgating this policy.
Repository	A location on the Verisign web site where DNSSEC related information is made accessible online.
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
Resource Record Signature (RRSIG)	Signature data in the zone file.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of the activation data needed to operate a private key under a Secret Sharing arrangement.
Signed-Key Response (SKR)	The output of a key signing ceremony, which contains all KSK signed ZSKs.
Supersede	A key is superseded when it stops being published in its respective zone.
SysTrust Assurance	SysTrust is an assurance service developed by American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

	SysTrust is designed primarily to build trust and confidence among businesses depending on systems, addressing areas such as: security, availability, confidentiality, and processing integrity.
Supplemental Risk	A review of an entity by Verisign following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Trusted Anchor	A trust anchor is an authoritative entity represented via a public key. It is used in the context of public key infrastructures, X.509 digital certificates and DNSSEC.
Trusted Role	The roles within the DNSSEC operations that must be held by a Trusted Person.
Trusted Persons	Persons who hold positions within DNSSEC operations.
Verisign	Means, with respect to each pertinent portion of this, VeriSign, Inc. and/or any wholly owned Verisign subsidiary responsible for the specific operations at issue.
Zone	A boundary of responsibility for each domain.
Zone Signing Key (ZSK)	A key that signs the COM Zone.

Appendix B. Changes From Previous Version

Section	Description
Entire Document	Format changes for the fonts and headers. Modified the formatting of the page numbers in the footer.
Cover Page	Title page fonts updated Changed “Version 2.1” to “Version 2.2” Updated effective date Changed “Copyright 2018” to “Copyright 2024”
1.2	Changed Version “2.1” to “2.2”
5.1.3	Changed “For the current key size, primality testing of RSA parameters (p and q) will be performed to ensure with the probability of less than 2^{-100} that the numbers are not composite. “ to “For all RSA keys utilized for DNSSEC signing, Verisign shall obtain assurance of the validity of the public and private key as required by FIPS 186-5.”
5.2.1	Changed “FIPS 140-2 Level 4” to “FIPS 140-2 Level 3 or FIPS 140-3 Level 3 or above.”
5.2.9	Changed “smartcards” to “credentials”
6.4	Changed “KSK” to “ZSK”
6.9	Modified the format of this section to include a formatted table.
A.1	Modified the format of this section to include a formatted table. Updated acronyms and terms.

A.2	Modified the format of this section to include a formatted table. Updated terms and definitions.
Appendix B	Modified the format of this section to include a formatted table.

Appendix C. Acknowledgments

This document is originally a product of the Root DNSSEC Design Team convened between ICANN, Verisign and the U.S. Government back in 2009 that was written based on experience as well as the feedback from the Internet community. This document has been maintained by the Verisign DNSSEC Policy Management Authority since then.

Of particular note, the first edition of this document was principally authored by Tomofumi Okubo, Fredrik Ljunggren, Richard Lamb, and Jakob Schlyter.

Author's Address

The DNSSEC Practices Manager
Verisign DNSSEC Policy Management Authority
c/o VeriSign, Inc
12061 Bluemont Way
Reston, VA 20190
USA
+1 (703) 948-3200 (voice)
+1 (703) 421-4873 (fax)
dnspractices@verisign.com