

# Verisign DNSSEC Practice Statement for TLD/GTLD Zone

---

**Version: 1.9**

**Effective Date: August 10, 2023**

## Abstract

This document is the DNSSEC Practice Statement (DPS) for the TLD/GTLD Zones identified in the Verisign TLD/GTLD Zone Service Domains document. It states the practices and provisions that are employed in providing TLD/GTLD Zone signing and zone distribution functions, such as issuing, managing, changing, and distributing Domain Name System (DNS) keys, for the TLD/GTLD Zone service. Verisign is the delegated Registry Operator for the TLD/GTLD Zones listed in the Verisign TLD/GTLD Zone Service Domains document under contract with the Internet Corporation for Assigned Names and Numbers.

## Copyright Notice

Copyright © 2023 VeriSign, Inc. All rights reserved.

## Trademark Notice

VERISIGN is a registered trademark of VeriSign, Inc.

VeriSign, Inc.  
12061 Bluemont Way  
Reston, VA 20190 USA  
+1 (703) 948-3200  
<https://www.verisign.com/>

# Table of Contents

- 1 INTRODUCTION..... 7
  - 1.1 Overview ..... 7
  - 1.2 Document Name and Identification..... 7
  - 1.3 Community and Applicability ..... 7
    - 1.3.1 TLD/GTLD Zone Manager ..... 7
    - 1.3.2 TLD/GTLD Zone Administrator ..... 8
    - 1.3.3 TLD/GTLD Zone Maintainer..... 8
    - 1.3.4 TLD/GTLD Server Operator ..... 8
    - 1.3.5 TLD/GTLD Zone Key Signing Key Operator ..... 8
    - 1.3.6 TLD/GTLD Zone Zone Signing Key Operator..... 8
    - 1.3.7 Child Zone Manager ..... 8
  - 1.4 Specification Administration..... 9
    - 1.4.1 Specification Administration Organization ..... 9
    - 1.4.2 Contact Information..... 9
    - 1.4.3 Specification Change Procedures..... 9
- 2 PUBLICATION AND REPOSITORIES ..... 9
  - 2.1 Publication of Key Signing Keys..... 9
  - 2.2 Repositories ..... 10
  - 2.3 Access Controls on Repositories ..... 10
- 3 OPERATIONAL REQUIREMENTS ..... 10
  - 3.1 Meaning of Domain Names ..... 10
  - 3.2 Activation of DNSSEC for Child Zone..... 10
  - 3.3 Identification and Authentication of Child Zone Manager ..... 10
  - 3.4 Registration of Delegation Signer Records ..... 10
  - 3.5 Removal of Delegation Signer Records ..... 10
- 4 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ..... 10
  - 4.1 Physical Controls..... 10
    - 4.1.1 Site Location and Construction ..... 11
    - 4.1.2 Physical Access..... 11
    - 4.1.3 Power and Air Conditioning ..... 11
    - 4.1.4 Water Exposures ..... 11

4.1.5	Fire Prevention and Protection .....	11
4.1.6	Media Storage .....	11
4.1.7	Waste Disposal .....	12
4.1.8	Off-Site Backup .....	12
4.2	Procedural Controls .....	12
4.2.1	Trusted Persons .....	12
4.2.2	Number of Persons Required Per Task .....	12
4.2.3	Identification and Authentication for Each Role .....	13
4.2.4	Tasks Requiring Separation of Duties.....	13
4.3	Personnel Controls.....	13
4.3.1	Qualifications, Experience, and Clearance Requirements .....	13
4.3.2	Background Check Procedures.....	13
4.3.3	Training Requirements.....	14
4.3.4	Retraining Frequency and Requirements .....	14
4.3.5	Job rotation Frequency and Sequence.....	14
4.3.6	Sanctions for Unauthorized Actions.....	14
4.3.7	Contracting Personnel Requirements .....	15
4.3.8	Documentation Supplied to Personnel .....	15
4.4	Audit Logging Procedures .....	15
4.4.1	Types of Events Recorded .....	15
4.4.2	Frequency of Processing Logs .....	16
4.4.3	Retention Period for Audit Logs.....	16
4.4.4	Protection of Audit Logs.....	16
4.4.5	Audit Logs Backup Procedures.....	16
4.4.6	Audit Collection System .....	16
4.4.7	Notification to Event-Causing Subject .....	16
4.4.8	Vulnerability Assessments .....	17
4.5	Compromise and Disaster Recovery .....	17
4.5.1	Incident and Compromise Handling Procedures .....	17
4.5.2	Corrupted Computing Resources, Software, and/or Data .....	17
4.5.3	Entity Private Key Compromise Procedures .....	17
4.5.4	Business Continuity and IT Disaster Recovery Capabilities .....	17
4.6	Entity Termination .....	18

5	TECHNICAL SECURITY CONTROLS .....	18
5.1	Key Pair Generation and Installation .....	18
5.1.1	Key Pair Generation .....	18
5.1.2	Public Key Delivery.....	19
5.1.3	Public Key Parameters Generation and Quality Checking .....	19
5.1.4	Key Usage Purposes .....	19
5.2	Private Key Protection and Cryptographic Module Engineering Controls .....	19
5.2.1	Cryptographic Module Standards and Controls.....	19
5.2.2	Private Key (M-of-N) Multi-Person Control.....	19
5.2.3	Private Key Escrow .....	19
5.2.4	Private Key Backup.....	20
5.2.5	Private Key Storage .....	20
5.2.6	Private Key Archival .....	20
5.2.7	Private Key Transfer In or Out of a Hardware Security Module.....	20
5.2.8	Method of Activating Private Key .....	20
5.2.9	Method of Deactivating Private Key .....	20
5.2.10	Method of Destroying Private Key.....	20
5.3	Other Aspects of Key Pair Management .....	21
5.3.1	Public Key Archival .....	21
5.3.2	Key Usage Periods.....	21
5.4	Activation Data .....	21
5.4.1	Activation Data Generation and Installation.....	21
5.4.2	Activation Data Protection.....	21
5.5	Computer Security Controls.....	21
5.6	Network Security Controls .....	21
5.7	Timestamping .....	22
5.8	Life Cycle Technical Controls.....	22
5.8.1	System Development Controls.....	22
5.8.2	Security Management Controls .....	22
5.8.3	Life Cycle Security Controls .....	22
6	ZONE SIGNING .....	22
6.1	Key Lengths, Key Types, and Algorithms.....	23
6.2	Authenticated Denial of Existence .....	23

6.3	Signature Format .....	23
6.4	Key Signing Key Rollover .....	23
6.5	Zone Signing Key Rollover .....	24
6.6	Signature Life-Time and Re-Signing Frequency.....	24
6.7	Verification of Zone Signing Key Set .....	25
6.8	Verification of Resource Records.....	25
6.9	Resource Records' Time-to-Live.....	25
7	COMPLIANCE AUDIT .....	26
7.1	Frequency of Entity Compliance Audit.....	26
7.2	Identity/Qualifications of Auditor .....	26
7.3	Auditor's Relationship to Audited Party .....	26
7.4	Topics Covered by Audit .....	26
7.5	Actions Taken as a Result of Deficiency .....	26
7.6	Communication of Results .....	26
8	LEGAL MATTERS.....	27
8.1	Fees .....	27
8.2	Financial Responsibility.....	27
8.3	Confidentiality of Business Information.....	27
8.3.1	Scope of Confidential Information .....	27
8.3.2	Types of Information Not Considered Confidential .....	27
8.3.3	Responsibility to Protect Confidential Information .....	27
8.4	Privacy of Personal Information.....	27
8.4.1	Information Treated as Private .....	27
8.4.2	Information Not Deemed Private .....	28
8.4.3	Responsibility to Protect Private Information.....	28
8.4.4	Disclosure Pursuant to Judicial or Administrative Process .....	28
8.5	Limitations of Liability .....	28
8.5.1	Dispute Resolution Provisions.....	28
8.5.2	Governing Law .....	28
8.6	Term and Termination .....	28
8.6.1	Term.....	28
8.6.2	Termination.....	28
Appendix A	Table of Acronyms and Terms.....	29

A.1 Acronyms.....	29
A.2 Terms.....	30
Appendix B Changes From Previous Version .....	31

# 1 INTRODUCTION

This document is the Verisign DPS for the TLD/GTLD Zone. It states the practices and provisions that are employed in providing TLD/GTLD Zone signing and zone distribution functions, such as issuing, managing, changing, and distributing DNS keys, for the TLD/GTLD 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 the DNS. DNSSEC provides a way for software to validate that DNS data have not been modified during Internet transit. This is done by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating at the Internet root.

DNS was not originally designed with strong security mechanisms to provide origin authentication, data integrity, and authenticated denial of existence of DNS data. 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 origin authentication, data integrity and authenticated denial of existence capabilities to the DNS.

This DPS is specifically applicable to all DNSSEC related operations performed by Verisign for the TLD/GTLD Zone. More generally, this document will provide the governing policies and provisions as they relate to the management, security, and technical specifications of the TLD/GTLD Zone Key Signing Key (KSK) and Zone Signing Key (ZSK). This document is under the control and management of Verisign. Information in this document and subsequent documents may be made public as required.

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

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

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

## 1.2 Document Name and Identification

Verisign DNSSEC Practice Statement for TLD/GTLD Zone

## 1.3 Community and Applicability

### 1.3.1 TLD/GTLD Zone Manager

The TLD/GTLD Zone manager is Verisign.

### **1.3.2 TLD/GTLD Zone Administrator**

The TLD/GTLD Zone administrator is Verisign.

### **1.3.3 TLD/GTLD Zone Maintainer**

The TLD/GTLD Zone maintainer is Verisign.

### **1.3.4 TLD/GTLD Server Operator**

The TLD/GTLD Zone operator is Verisign.

### **1.3.5 TLD/GTLD Zone Key Signing Key Operator**

The TLD/GTLD Zone KSK operator is Verisign. The TLD/GTLD Zone KSK operator is responsible for:

- 1) generating and protecting the private component of the TLD/GTLD KSK,
- 2) securely importing public key components from the TLD/GTLD Zone ZSK operator,
- 3) authenticating and validating the public TLD/GTLD ZSK keyset,
- 4) securely signing the TLD/GTLD KSK and ZSK keyset (i.e., all DNSKEY records),
- 5) securely exporting the TLD/GTLD KSK public key components,
- 6) securely transmitting the signed TLD/GTLD DNSKEY resource record set (RRset) to the TLD/GTLD Zone ZSK operator,
- 7) creating a Delegation Signer (DS) record from the KSK public key and preparing it for the TLD/GTLD registry of record,
- 8) The TLD/GTLD registry of record will submit this to IANA for insertion into the Root Zone, and
- 9) issuing an emergency key rollover within a reasonable amount of time if any KSK associated with the zone is lost or suspected by Verisign to be compromised.

### **1.3.6 TLD/GTLD Zone Zone Signing Key Operator**

The TLD/GTLD Zone ZSK operator is Verisign. The TLD/GTLD Zone ZSK operator is responsible for:

- 1) generating and protecting the private component of the TLD/GTLD ZSK,
- 2) securely exporting and transmitting the public TLD/GTLD ZSK component to the TLD/GTLD Zone KSK operator,
- 3) securely importing the signed TLD/GTLD DNSKEY RRset from the TLD/GTLD Zone KSK operator,
- 4) signing the TLD/GTLD Zone's authoritative resource records omitting the DNSKEY RRset, and
- 5) issuing an emergency key rollover within a reasonable amount of time if any ZSK associated with the zone is lost or suspected by Verisign to be compromised.

### **1.3.7 Child Zone Manager**

The child zone managers are trustees for the delegated domain, and as such are responsible for providing their own DNS services and operating subordinate DNS servers. In regard to DNSSEC, the child zone manager is also responsible for:

- 1) generating the keys associated with the zone using a trustworthy method,
- 2) registering and maintaining the shorthand representations of its KSK (in the form of a 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 the zone, and
- 4) issuing an emergency key rollover within a reasonable amount of time if any key associated with the zone is lost or suspected to be compromised.

## 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 this DPS and should be considered as the point of contact for all matters related to this 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](mailto:dnspractices@verisign.com)

### 1.4.3 Specification Change Procedures

Amendments to this DPS are made by the PMA. Amendments will be in the form of either a document containing an amended form of this DPS or an update. Amended versions and updates will be linked to the DNSSEC Practices Updates and Notices section of the Verisign Repository located at: [https://www.verisign.com/en\\_US/repository/index.xhtml](https://www.verisign.com/en_US/repository/index.xhtml). Updates supersede any designated or conflicting provisions of the referenced version of this DPS. Verisign and the PMA reserve the right to amend this DPS without notification.

The PMA may solicit proposed amendments to this DPS from other Verisign subdomain participants. If the PMA considers such an amendment desirable, the PMA will approve the proposed amendment and the amended form of this DPS will be uploaded to the Verisign Repository. Notwithstanding anything in this DPS to the contrary, if the PMA believes that amendments to this DPS are immediately necessary to stop or prevent a breach of security, Verisign and the PMA are entitled to make such amendments that are effective immediately upon approval by the PMA.

## 2 PUBLICATION AND REPOSITORIES

### 2.1 Publication of Key Signing Keys

A hash of the public portion of the TLD/GTLD KSK will be published in the Root Zone.

## 2.2 Repositories

Verisign publishes this DPS, and the Verisign TLD/GTLD Zone Service Domains document, in the repository section of Verisign's web site at: [https://www.verisign.com/en\\_US/repository/index.xhtml](https://www.verisign.com/en_US/repository/index.xhtml).

## 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

DNSSEC provides mechanisms for ensuring that the origin of the DNS data is consistent with the information in the registry. DNSSEC does not provide any way of determining the legal entity behind the domain name, or the relevance of the domain name itself.

## 3.2 Activation of DNSSEC for Child Zone

DNSSEC for a child zone is activated by the publication of a signed DS record for that child zone in the TLD/GTLD Zone. The DS record is a cryptographic shorthand representation, or hash, of the public portion of the child zone generated and controlled KSK. The DS record establishes a chain of trust from the TLD/GTLD Zone to the child zone.

## 3.3 Identification and Authentication of Child Zone Manager

Verisign does not validate the identity and authority of any child zone manager.

## 3.4 Registration of Delegation Signer Records

Verisign applies changes to the TLD/GTLD Zone file based on requests from registrars.

## 3.5 Removal of Delegation Signer Records

Verisign's removal of DS records (stale or active) can only be requested by registrars.

# 4 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 4.1 Physical Controls

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's Physical Security Policy contains confidential 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 TLD/GTLD KSK and ZSK occurs 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. The physical security system includes additional tiers for key management security, which serve 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 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 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 measures 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 and logical 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 Persons

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 TLD/GTLD Zone KSK,
- secure export or import of any public components, or
- generation and signing of zone file data.

Trusted Persons include, but are not limited to:

- Naming Provisioning and Resolution Operations personnel,
- Cryptographic Business Operations (CBO) personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives who are designated to manage infrastructural trustworthiness.

Verisign considers the categories of personnel identified in this section as Trusted Persons. Personnel seeking to become Trusted Persons 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 (e.g., 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 both physical and

logical access to the cryptographic hardware device. Persons with physical access to HSMs do not hold Secret Shares and vice versa.

### **4.2.3 Identification and Authentication for Each Role**

For all personnel seeking to become a Trusted Person, 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 Person status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities, or
- issued electronic credentials to access and perform specific functions on applicable Verisign IT (Information Technology) 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 TLD/GTLD Zone DNSSEC key material.

Designated third-party audit personnel may not participate in the multi-person control for the TLD/GTLD KSK or ZSK.

## **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 or proof of any citizenship necessary to perform operations under government contracts.

### **4.3.2 Background Check Procedures**

All personnel with access to any cryptographic component used with the TLD/GTLD 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 that 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 a candidate for a Trusted Person 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.

Verisign's human resources and security personnel evaluate reports containing such information and 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 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, and
- disaster recovery and business continuity procedures.

### **4.3.4 Retraining Frequency and Requirements**

Verisign provides refresher training and updates to 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**

Personnel 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 under Verisign's direct supervision. 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 that 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 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:

TLD/GTLD KSK and ZSK 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.

TLD/GTLD KSK and ZSK signing and management events, including:

- key activation,
- receipt and validation of signed public key material,
- successful and unsuccessful signing requests, and
- key rollover events.

TLD/GTLD KSK and ZSK security-related events, including:

- successful and unsuccessful system access attempts,
- secure cryptographic actions performed by Trusted Persons,
- security sensitive files and 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 related to logged events,
- type of event, and

- other events as appropriate.

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

#### **4.4.2 Frequency of Processing Logs**

Audit logs are examined at least once 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 Logs**

All audit log data collected in terms of section 4.4.1 are retained on-site for at least one year after creation and are thereafter archived for at least two 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 Logs**

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 Logs Backup Procedures**

Verisign incrementally backs up electronic archives of its TLD/GTLD KSK and ZSK information on a daily basis and performs full backups on a weekly basis. Copies of any paper-based records are maintained in a secure facility.

#### **4.4.6 Audit Collection System**

Automated audit data are 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 the archive. These backups are maintained in a 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, at minimum, to monitor for system vulnerabilities. Patches are applied, as necessary, in accordance with Verisign's Information Security Documentation.

### **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 KSK, the emergency KSK rollover procedure will be enacted. 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 Documentation. Such procedures require appropriate escalation, incident investigation and incident response.

#### **4.5.2 Corrupted Computing Resources, Software, and/or Data**

In the event of the corruption of computing resources, software, and/or data, Verisign's 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 private key compromise or disaster recovery procedures will be implemented.

#### **4.5.3 Entity Private Key Compromise Procedures**

##### **4.5.3.1 Key Signing Key Compromise**

Upon the suspected or confirmed compromise of the TLD/GTLD KSK, the Verisign Incident Response Team (IRT) implements Verisign's key compromise response procedures. This team, which includes Information Security, CBO, Production Services personnel, and other Verisign management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from Verisign executive management.

##### **4.5.3.2 Zone Signing Key Compromise**

Upon the suspected or confirmed compromise of the TLD/GTLD ZSK, the IRT implements Verisign's key compromise response procedures. This team, which includes Information Security, CBO, Production Services personnel, and other Verisign management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from Verisign executive management.

#### **4.5.4 Business Continuity and IT Disaster Recovery Capabilities**

Verisign has implemented a secure disaster recovery site that is physically and geographically separate from Verisign's principal secure facility. Verisign has developed, implemented and tested business continuity and IT disaster recovery plans to mitigate the effects of natural, man-made, or technological disasters. Detailed

business continuity and IT 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) that 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 Cryptographic 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. Verisign has the capability to restore or recover essential operations following a recovery event with, at a minimum, support for the following functions:

- communication with the public,
- ability to import and export Key Signing Requests (KSR),
- generation of KSKs,
- generation of ZSKs,
- processing and signing of KSR contents,
- signing of a zone file, and
- distribution of the signed zone file.

Verisign's disaster recovery environment is protected by physical security controls comparable to the physical security tiers specified in DPS section 4.1.2. Verisign's business continuity and IT disaster recovery plans have been designed to provide full recovery of critical functionality following any incident or disaster occurring at Verisign's primary site. Verisign tests its environment at its primary site to support all functions to include DNSSEC functions following all but a major disaster that would render the entire facility inoperable. 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

In the event that the TLD/GTLD Zone manager is required to change to another party, Verisign will coordinate with all required parties in order to execute the transition in a secure and transparent manner.

# 5 TECHNICAL SECURITY CONTROLS

## 5.1 Key Pair Generation and Installation

### 5.1.1 Key Pair Generation

TLD/GTLD Zone KSK and ZSK key pair generations are performed by multiple pre-selected, trained, and trusted individuals using secured systems and processes that provide for the security and required cryptographic strength for the generated keys. The HSMs used for TLD/GTLD KSK or ZSK key generations meet the requirements of Federal Information Processing Standards (FIPS) 140-2 level 3.

All KSK and ZSK key pairs are generated in pre-planned Cryptographic Key Generation Ceremonies in accordance with the requirements of the Cryptographic Key Ceremony Guide and the Verisign Information and Physical Security Policies. The activities performed in each Cryptographic Key Generation Ceremony are

recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Verisign Management.

### **5.1.2 Public Key Delivery**

Public key information about the KSKs comes in the Signed-Key Response (SKR) XML from the CBO. Public key information for the ZSKs comes locked inside of the HSMs that are delivered to the data centers by CBO personnel.

### **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.

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

### **5.1.4 Key Usage Purposes**

Any TLD/GTLD Zone KSK or ZSK private key will be used only for signing the relevant TLD/GTLD Zone's RRsets or self-signing its own DNSKEY RRsets to provide proof of possession of the private key.

## **5.2 Private Key Protection and Cryptographic Module Engineering Controls**

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

### **5.2.1 Cryptographic Module Standards and Controls**

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

### **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 a TLD/GTLD KSK or 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. The threshold number is required to activate a TLD/GTLD KSK or ZSK private key stored on the HSM. The threshold number of shares needed is three.

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.

### **5.2.3 Private Key Escrow**

Private components of TLD/GTLD KSK and ZSK are not escrowed.

## 5.2.4 Private Key Backup

Verisign creates backup copies of TLD/GTLD KSK and 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. HSMs containing on-site backup copies of TLD/GTLD KSK and ZSK private keys are subject to the requirements of this DPS. HSMs containing disaster recovery copies of TLD/GTLD KSK and ZSK private keys are subject to the requirements of this DPS.

## 5.2.5 Private Key Storage

Private keys held on HSMs are stored in encrypted form.

## 5.2.6 Private Key Archival

TLD/GTLD KSK and 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. Decommissioned HSMs will be zeroized and/or physically destroyed when possible.

## 5.2.7 Private Key Transfer In or Out of a Hardware Security Module

Verisign generates TLD/GTLD KSK and ZSK key pairs on the HSMs, in which the keys will be used, with replication procedures for copying those same keys onto backups (in the case of the KSK) and onto copies used for live signing (in the case of the ZSKs). 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

TLD/GTLD KSK and ZSK private keys will be set to an activated state using a minimum of three Secret Shares.

## 5.2.9 Method of Deactivating Private Key

TLD/GTLD KSK and ZSK private keys are set to an inactive state upon system shutdown.

## 5.2.10 Method of Destroying Private Key

Where required, Verisign destroys the TLD/GTLD KSK and 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, if able, of its HSM and other appropriate means to ensure the complete destruction of TLD/GTLD KSK and 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

TLD/GTLD KSK and ZSK public keys are backed up and archived.

### 5.3.2 Key Usage Periods

The operational period of each TLD/GTLD KSK and ZSK ends upon its supersession. The superseded TLD/GTLD KSK and ZSK are 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 Verisign TLD/GTLD KSK and ZSK private keys are generated in accordance with the requirements of DPS section 5.2. The creation and distribution of Secret Shares is logged.

When required, activation data for the TLD/GTLD HSMs are transmitted from the PIN Entry Device to the HSM. This transmission occurs on Verisign's secure infrastructure.

### 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 TLD/GTLD KSK and ZSK private keys will be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, and unauthorized use of the private keys protected by such activation data. Verisign will decommission Secret Shares by zeroizing and/or physical destruction after decommissioning the associated HSMs.

## 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 software 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 an event.

Time derived from the procedure will be used for timestamping of

- electronic and paper-based audit log records, and
- DNSSEC signature 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 packaging to their destination in the secure facility. Any hardware will be decommissioned prior to its specified life expectancy.

## 6 ZONE SIGNING

The TLD/GTLD Zone manager provides the TLD/GTLD Zone maintainer with a signed and valid DNSKEY RRset containing the TLD/GTLD Zone ZSK operator's current keys and the KSKs.

Depending on the TLD/GTLD that is implemented, one of the two options will be used:

Option 1: The TLD/GTLD Zone maintainer includes this keyset into the TLD/GTLD Zone file, adds the Next Secure 3 (NSEC3) Records and creates signatures for all relevant records. The TLD/GTLD Zone is then distributed to the TLD/GTLD server operators.

Option 2: The TLD/GTLD Zone maintainer includes this keyset into the TLD/GTLD Zone file, adds the Next Secure (NSEC) Records and creates signatures for all relevant records. The TLD/GTLD Zone is then distributed to the TLD/GTLD Server Operators.

The TLD/GTLD Zone maintainer will conduct the continuous TLD/GTLD Zone signing automatically.

## 6.1 Key Lengths, Key Types, 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 TLD/GTLD Zone uses either DNSSEC algorithm 8 (RSA/SHA-256) or DNSSEC algorithm 13 (ECDSA Curve P-256 with SHA-256) keys, or both (e.g., during an algorithm rollover).

A TLD/GTLD algorithm 8 KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits.  
A TLD/GTLD algorithm 8 ZSK key pair(s) is an RSA key pair, with a modulus size of at least 1024 bits.

TLD/GTLD Zone algorithm 13 KSKs and ZSKs are ECDSA Curve P-256 key pairs.

## 6.2 Authenticated Denial of Existence

Depending on the TLD/GTLD that it is implemented, one of the two options will be used:

Option 1: Authenticated denial of existence will be provided through the use of NSEC3 records as specified in Request for Comments (RFC) 5155.

Option 2: Authenticated denial of existence will be provided through the use of NSEC records as specified in RFC 4034.

## 6.3 Signature Format

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

Depending on the TLD/GTLD that it is implemented, one of the two options will be used:

Option 1: The TLD/GTLD KSK and ZSK signatures will be generated by encrypting SHA-256 hashes.

Option 2: The TLD/GTLD KSK and ZSK signatures will be generated by encrypting SHA-512 hashes.

## 6.4 Key Signing Key Rollover

Currently there are no definite planned TLD/GTLD KSK rollovers, but Verisign will assess the need for a TLD/GTLD KSK rollover approximately once a year.

## 6.5 Zone Signing Key Rollover

TLD/GTLD ZSK rollover is automatically carried out quarterly by the system. TLD/GTLD ZSK key signing is conducted in advance (so as to keep the TLD/GTLD KSK offline as much as possible). The necessary TLD/GTLD ZSKs, to be used in between the signing ceremonies, are pre-generated and signed at the same occasion with the projected signature inception and expiration time. In extraordinary circumstances, such as when changing key lengths or algorithms, rollovers may occur outside of the quarterly schedule.

## 6.6 Signature Life-Time and Re-Signing Frequency

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

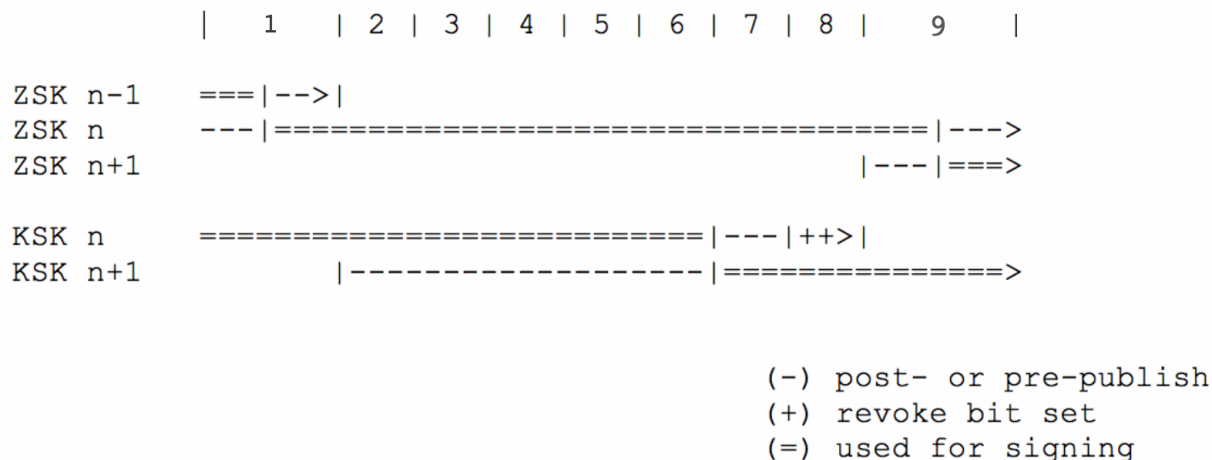
January 15  
 April 15  
 July 15  
 October 15

If the time cycle is more than 90 days, the last slot in the cycle will be expanded to fill the period. An out-of-schedule ZSK rollover may occur in emergency situations or extraordinary circumstances (such as when changing key lengths or algorithms). An out-of-schedule rollover will have a shorter-than-normal time cycle.

Any resulting resource record signature (RRSIG) record generated by the KSK will not have a validity period longer than 15 days and are pre-generated up to 18 months in advance. Any resulting RRSIG record generated by the ZSK will not have a validity period longer than 7 days and will not extend more than 7 days into the future.

All DNSKEY records produced by the changes as described in section 6.5 are known in advance and signed in advance by the TLD/GTLD KSK. The collection of DNSKEY records for which Verisign pre-generates digital signatures span a period of one year or more from the beginning of the first signature inception date.

A new ZSK is generated by the TLD/GTLD Zone ZSK Operator to be used for each new time cycle. Hence, a TLD/GTLD ZSK rollover is performed at the edge of every time cycle. 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 a ZSK is used for signing in more than one time cycle.



Quarterly cycle with KSK and ZSK rollover

Figure 1

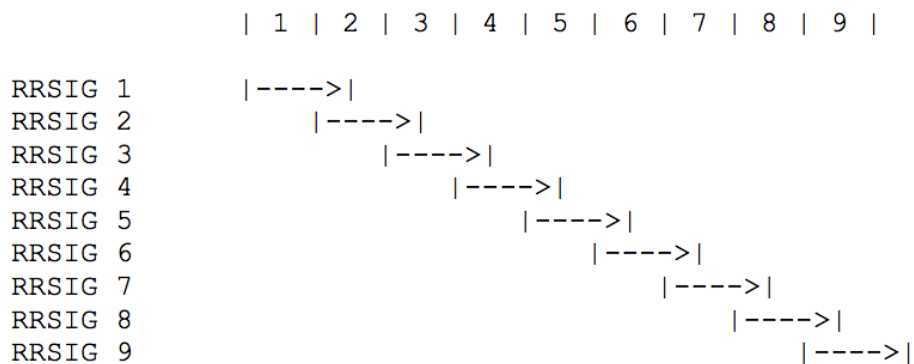


In the event of a ZSK rollover, time slots are used for pre-publish and post-publish in the following order;

- Slot 1:  
Publish ZSK (n) + ZSK (n-1) + KSK, 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 TLD/GTLD Zone maintainer selects and includes the current DNSKEY RRset and corresponding signature(s), and then signs all other authoritative records within the TLD/GTLD Zone using the current TLD/GTLD ZSK with a validity period set to seven days.

For each of these slots there is a pre-generated DNSKEY key set that is signed at a key ceremony.



DNSKEY RRSIG's validity period within the cycle

Figure 2

## 6.7 Verification of Zone Signing Key Set

The TLD/GTLD Zone KSK operator's system will verify that the signature data are authentic by validating the public key data contained in the KSR.

## 6.8 Verification of Resource Records

The extractor/validator system verifies all RRSIGs prior to distribution. The integrity of the unsigned zone contents is also validated prior to distribution.

## 6.9 Resource Records' Time-to-Live

RR Type	Time-To-Live (TTL)
DNSKEY	24 hours
DS	24 hours
NSEC3	Same as the minimum TTL value field in the zone SOA RR
RRSIG	same as the covered RRset (varies to a maximum of 48 hours)

## **7 COMPLIANCE AUDIT**

An annual compliance audit for DNSSEC operations examination is performed for Verisign's data center operations and key management operations supporting Verisign's TLD/GTLD Zone signing services including the TLD/GTLD KSK and 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 TLD/GTLD KSK and 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, TLD/GTLD KSK and 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 TLD/GTLD KSK and/or 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 Verisign's Management Assertion can be found at [https://www.verisign.com/en\\_US/repository/index.xhtml](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 following records shall be kept confidential and private:

- private keys and information needed to recover such private keys,
- transactional records (both full records and the audit trail of transactions),
- audit trail records created or retained by Verisign,
- Information Security related documents,
- audit reports created by Verisign (to the extent such reports are maintained) or their respective auditors (whether internal or public);
- contingency planning and disaster recovery plans, and
- security measures controlling the operations of Verisign hardware and software and the administration of DNS keys.

#### **8.3.2 Types of Information Not Considered Confidential**

All information pertaining to the database of top-level domains is public information. Public keys and other status information, as well as Verisign repositories and information contained within them are not considered confidential/private information.

#### **8.3.3 Responsibility to Protect Confidential Information**

Verisign secures confidential information against compromise and disclosure to third parties.

### **8.4 Privacy of Personal Information**

#### **8.4.1 Information Treated as Private**

To the extent, Verisign receives or processes, on behalf of a customer, Personal Identifiable Information (PII) in the course of providing TLD/GTLD Zone services, such PII is treated as private, subject to applicable law, by the applicable customer agreement and to the extent not governed by any applicable customer agreement, by Verisign's Privacy Policy as set forth at [https://www.verisign.com/en\\_US/privacy/index.xhtml](https://www.verisign.com/en_US/privacy/index.xhtml).

## **8.4.2 Information Not Deemed Private**

Subject to applicable laws, all information required to be published as part of a whois database is deemed not private.

## **8.4.3 Responsibility to Protect Private Information**

In providing TLD/GTLD Zone services, any obligations that Verisign may have with respect to any PII is governed, subject to applicable law, by the applicable customer agreement and to the extent not governed by any applicable customer agreement, by Verisign's Privacy Policy set forth at [https://www.verisign.com/en\\_US/privacy/index.xhtml](https://www.verisign.com/en_US/privacy/index.xhtml).

## **8.4.4 Disclosure Pursuant to Judicial or Administrative Process**

Verisign shall be entitled to disclose confidential/private Information if, in good faith, Verisign believes that disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

## **8.5 Limitations of Liability**

Verisign shall not be liable for any financial loss or loss arising from incidental damage or impairment resulting from its performance of its obligations hereunder or the TLD/GTLD Zone manager's or the TLD/GTLD Zone KSK and ZSK operator's performance of their respective obligations under this DPS for the TLD/GTLD Zone KSK and ZSK operator. No other liability, implicit or explicit, is accepted.

### **8.5.1 Dispute Resolution Provisions**

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties. Disputes involving Verisign require an initial negotiation period of 60 days followed by litigation in the federal or state court encompassing Fairfax County, Virginia.

### **8.5.2 Governing Law**

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

## **8.6 Term and Termination**

### **8.6.1 Term**

This DPS becomes effective upon publication in the Verisign Repository. Amendments to this DPS become 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.

## Appendix A Table of Acronyms and Terms

### A.1 Acronyms

<b>Acronym</b>	<b>Term</b>
AICPA	American Institute of Certified Public Accountants
CBO	Cryptographic Business Operations
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPS	DNSSEC Practice Statement
DS	Delegation Signer
ECDSA	Elliptical Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GTLD	Generic Top Level Domain
HSM	Hardware Security Module
KSK	Key Signing Key
KSR	Key Signing Request
NSEC3	NextSecure3
NTP	Network Time Protocol
PII	Personal Identifiable Information
PMA	Policy Management Authority
RFC	Request for Comments
RRSIG	Resource Record Signature
SHA	Secure Hash Algorithm
SKR	Signed-Key Response
SOA	Start of Authority
TLD	Top Level Domain
TTL	Time-To-Live
IRT	Verisign Incident Response Team
ZSK	Zone Signing Key

## A.2 Terms

<b>Term</b>	<b>Definition</b>
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.
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.
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.
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 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.
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.
Supersedence	A key is superseded when it stops being published in its respective zone.
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 TLD/GTLD Zone.

## Appendix B Changes From Previous Version

### Changes from Previous Version: Version 1.8

Section	Description
Cover Page	Changed version from 1.8 to 1.9 Updated copyright from 2019 to 2023
5.1.3	<p>Changed “For the current ZSK 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.</p> <p>For all ECDSA keys utilized for DNSSEC signing, Verisign shall obtain assurance of the validity of the domain parameters as well as the public and private keys as required by FIPS 186-5.”</p>
6.1	<p>Changed “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.</p> <p>The COM Zone uses either DNSSEC algorithm 8 (RSA/SHA-256) or DNSSEC algorithm 13 (ECDSA Curve P-256 with SHA-256) keys, or both (e.g., during an algorithm rollover).</p> <p>A TLD/GTLD algorithm 8 KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits. A TLD/GTLD algorithm 8 ZSK key pair(s) is an RSA key pair, with a modulus size of at least 1024 bits.” to “The TLD/GTLD Zone uses either DNSSEC algorithm 8 (RSA/SHA-256) or DNSSEC algorithm 13 (ECDSA Curve P-256 with SHA-256) keys, or both (e.g., during an algorithm rollover).</p> <p>A TLD/GTLD algorithm 8 KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits. A TLD/GTLD algorithm 8 ZSK key pair(s) is an RSA key pair, with a modulus size of at least 1024 bits.</p> <p>TLD/GTLD Zone algorithm 13 KSKs and ZSKs are ECDSA Curve P-256 key pairs.”</p>
Appendix A.1	Added acronym ECDSA – Elliptical Curve Digital Signature Algorithm
Appendix B	Changed “1.7” to “1.8”