Verisign DNSSEC Practice Statement for TLD/GTLD Zone

Version 1.3

Effective Date: December 1, 2015

Abstract

This document is the DNSSEC Practice Statement for the TLD/GTLD Zone. It states the practices and provisions that are employed in providing TLD/GTLD Zone Signing and Zone distribution services that include, but are not limited to, issuing, managing, changing, and distributing DNS keys. Verisign is the delegated registry operator for the TLD/GTLD zone under contract with the Internet Corporation for Assigned Names and Numbers.

VeriSign, Inc.
12061 Bluemont Way
Reston, VA 20190 USA
+1 (703) 948-3200
http://www.verisigninc.com

Table of Contents

1.
INTRODUCTION

This document is the Verisign DNSSEC Practice Statement (DPS) for the TLD/GTLD zone. It states the practices and provisions that Verisign employs in providing TLD/GTLD zone signing and distribution services that include, but are not limited to, issuing, managing, changing and distributing DNS keys.

1.1. Overview

The Domain Name System Security Extensions (DNSSEC) is a set of IETF specifications for adding origin authentication and data integrity to the Domain Name System. DNSSEC provides a way for software to validate that Domain Name System (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 integrity and authenticity 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 data origin authentication, data integrity verification 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 Key Signing Key and Zone Signing Key. 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 TLD/GTLD KSK and 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
- The Verisign Information Security Policy – Describes telecommunications and logical security requirements
- The Verisign Cryptographic Key Management Guide – Describes cryptographic key management security
- The Verisign Key Ceremony Guide – Describes the procedures used to generate cryptographic keys

In many instances, the DPS refers to these ancillary documents for specific, detailed practices implementing Verisign proprietary standards where including the specifics in the DPS could compromise the security of the TLD/GTLD zone signing operation.

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. This role differs from the third party auditors who conduct the compliance audit and generate the audit report.

1.3.3. TLD/GTLD Zone Maintainer

The TLD/GTLD Zone Maintainer is Verisign performing the function of receiving change requests to the TLD/GTLD Zone, implementing the changes, generating a new TLD/GTLD Zone File and publishing the TLD/GTLD Zone.

1.3.4. TLD/GTLD Server Operators

Verisign serves as the only operator for the TLD/GTLD zone.

1.3.5. TLD/GTLD Zone Key Signing Key Operator

The TLD/GTLD Zone Key Signing Key Operator is Verisign performing the function of generating the TLD/GTLD Zone's Key Signing Key (KSK) and signing the TLD/GTLD keyset using the KSK. The TLD/GTLD Zone Key Signing Key Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the Key Signing Key to the parent zone.

The TLD/GTLD Zone KSK (TLD/GTLD 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 Zone Signing Key (ZSK) operator.
3) Authenticating and validating the public TLD/GTLD ZSK keyset.
4) Securely signing the TLD/GTLD ZSK and KSK keyset (i.e., all DNSKEY records).
5) Securely transmitting the signed TLD/GTLD DNSKEY Resource-Record Set to the TLD/GTLD ZSK operator.
6) Securely exporting the TLD/GTLD KSK public key components.
7) Creating a 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.
9) Issuing an emergency key roll-over within reasonable time if any KSK associated with the zone is lost or suspected to be compromised.

1.3.6. TLD/GTLD Zone Zone Signing Key Operator

The TLD/GTLD Zone Zone Signing Key Operator is Verisign performing the function of generating the TLD/GTLD Zone's Zone Signing Key (ZSK) and signing the TLD/GTLD Zone File using the ZSK.

The TLD/GTLD Zone Zone Signing Key Operator is also responsible for securely generating and storing the private keys and distributing the public portion of the Zone Signing Key to the TLD/GTLD Zone Key Signing Key Operator for signing.

The TLD/GTLD Zone ZSK (TLD/GTLD 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 KSK Operator.
3) Securely importing the signed TLD/GTLD DNSKEY Resource Record Set from the TLD/GTLD KSK operator.
4) Signing the TLD/GTLD Zone's authoritative resource records omitting the DNSKEY resource record.
5) Issuing an emergency key roll-over within a reasonable amount of time if any ZSK associated with the zone is lost or suspected to be compromised.

1.3.7. Child zone manager

The child zone (TLD/GTLD Domain Name) 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 Key Signing Key (in the form of a Delegation Signer 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.
4) Issuing an emergency key roll-over within a reasonable 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 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.

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 be in the form of either a document containing an amended form of the 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: http://www.verisigninc.com/en_US/repository/index.xhtml. Updates supersede any designated or conflicting provisions of the referenced version of the DPS.

Verisign and the PMA reserve 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 DNSSEC Practices Updates and Notices section of the Verisign Repository, which is located at: http://www.verisigninc.com/en_US/repository/index.xhtml.

The PMA solicits proposed amendments to the DPS from other Verisign subdomain participants. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA will provide 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, Verisign and the PMA are 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 publishes the DPS in the repository section of Verisign's web site at http://www.verisigninc.com/en_US/repository/index.xhtml.

2.2. Publication of key signing keys

The public portion of the TLD/GTLD KSK will be published in the TLD/GTLD zone.

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. It 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 publishing in the TLD/GTLD zone of a signed DS record for that child zone. The DS record is a cryptographic shorthand representation, or hash, of the child zone generated and controlled Key Signing Key. It will establish 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 perform any verification of the identity and authority of the child zone manager as it only applies changes received from Registrars.

3.4. Registration of delegation signer (DS) records

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

3.5. Removal of DS record

3.5.1. Who can request removal

The removal of DS records (stale or active) can be requested by only the Child Zone manager.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

Verisign has implemented the Verisign Physical Security Policy, which supports the 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 sensitive security information and is available only upon agreement with Verisign. 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, any activity related to the lifecycle of the TLD/GTLD KSK & ZSK, occurs within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. The

physical security system includes additional tiers for key management security which serves to protect both online and offline storage of HSMs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online HSMs are protected through the use of locked cabinets. Offline HSMs are protected through the use of locked safes, cabinets 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 or containers in these tiers are 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 precautions 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, as well as media containing data, audit, archive, and backup information is 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 and materials 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 prior to disposal. Other waste is disposed of in accordance with Verisign's normal waste disposal requirements.

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 Verisign's East Coast disaster recovery facility.

4.2. Procedural Controls

4.2.1. Trusted roles

Trusted Persons include all employees, contractors, and consultants that have access to or control cryptographic operations that may materially affect:

- Generation and protection of the private component of the TLD/GTLD Zone Key Signing Key;
- Secure export or import of any public components; and
- Generation and 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 who 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 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. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities.

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

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

4.2.3. Identification and authentication for each role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Verisign Human Resource or security functions and a check of well-recognized forms of 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 Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities
- issued electronic credentials to access and perform specific functions on Verisign IT systems.

4.2.4. Tasks requiring separation of duties

Tasks requiring separation of duties include, but are not limited to, the generation, operation or destruction of

TLD/GTLD Zone DNSSEC key material.

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

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Verisign requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof 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 background check extending back at least three years.

Prior to commencement of employment in a Trusted Role, 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
- 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 Trusted Positions 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
- Certain criminal convictions

Reports containing such information are evaluated by Verisign's 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 Trusted Positions 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 are tailored to the individuals' responsibilities and 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

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 to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a Verisign employees in a comparable position. Independent contractors and consultants who have not completed or passed the background check procedures specified in DPS section 4.3 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 employees 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:

TLD/GTLD KSK & ZSK life cycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction
- Exporting of public key components
- Cryptographic device life cycle management events

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

- Key activation
- Receipt and validation of signed public key material
- Successful and unsuccessful signing requests
- Key rollover events

Security-related events, including:

- Successful and unsuccessful system access attempts
- Key and security system actions performed by trusted personnel
- Security sensitive files and records read, written and deleted
- Security profile changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- Facility visitor entry/exit
- System changes and maintenance/system updates
- Incident response handling

Log entries include the following elements:

- Date and time of the entry
- Identity of the entity making the journal entry
- Serial or sequence number of entry, for automatic journal entries
- Kind of entry
- Other events as appropriate

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

4.4.2. Frequency of processing log

Audit logs are examined after each key ceremony 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 consists of a review of the audit logs and documentation for all significant events. Audit log reviews include a verification that the log has not been tampered with and 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 data collected in terms of section 4.4.1 are retained on-site for at least one (1) year after creation and are thereafter archived for at least 2 years.

The media holding the audit 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.

4.4.5. Audit log backup procedures

Verisign incrementally backs up electronic archives of its TLD/GTLD ZSK and KSK information on a daily basis and performs full backups on a weekly basis. Copies of any paper-based records will be 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 audit data are recorded 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 the 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

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments ("SVAs") are performed, and reviewed following an examination of these monitored events. SVAs are based on automated logging data and are performed on a regular basis. An annual SVA will be an input into an entity's annual Compliance Audit.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

Backups of audit data and database records are kept in off-site storage and are available in the event of a compromise or disaster.

Back-ups of private keys will be generated and maintained in accordance with the DPS section 5.2.4.

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 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 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 known compromise of the TLD/GTLD Key Signing Key, Verisign's Key Compromise Response procedures are implemented by the Verisign Security Incident Response Team (VSIRT). This team, which includes Information Security, Cryptographic Business Operations, 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 known compromise of the TLD/GTLD Zone Signing Key, Verisign's Key Compromise Response procedures are implemented by the Verisign Security Incident Response Team (VSIRT). This team, which includes Information Security, Cryptographic Business Operations, 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 disaster recovery site that is physically and geographically separate from Verisign's principal secure facilities. Verisign has developed, implemented and tested business continuity and IT disaster recovery plans to mitigate the effects of natural, man-made, and technological disasters. These plans are regularly tested, validated, and updated to be operational in the event of any incident or disaster. 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 that is supported by a formal Corporate Incident Management Team (CIMT) and business unit 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 protections and operational controls required by Verisign Physical Security Policies, the Verisign Cryptographic Key Management Security Guide and the Verisign Key Ceremony Guide to provide for a secure and sound backup operational environment. In the event of a natural and man-made, or technological incident or disaster that requires temporary or permanent cessation of operations from Verisign's primary facility, Verisign's business continuity and IT disaster recovery process is initiated by the Verisign Incident Response Team (IRT) and Corporate Incident Management Team (CIMT). Verisign has the capability to restore or recover essential operations following a disaster with, at a minimum, support for the following functions:

- Communication with the public
- Ability to import and export KSRs
- Generation of Key Signing Keys
- Processing and signing of KSR contents
- Signing of a Zone File
- Distribution of the Signed Zone File
- Generation of Zone Signing Keys

Verisign's disaster recovery environment is synchronized regularly with the production system within the time limits set forth in the Verisign Information and Physical Security Policies. Verisign's disaster recovery environment is protected by physical security protections 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. Where 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 adopted a DNSSEC termination plan in the event that the roles and responsibilities of the TLD/GTLD Zone ZSK and KSK Operator must transition to other entities. Verisign will co-ordinate 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 (TLD/GTLD) Key Signing Key (KSK) and Zone Signing Key (ZSK) key pair generation are performed by multiple pre-selected, trained, and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for TLD/GTLD KSK & ZSK key generation meet the requirements of FIPS 140-2 level 3.

All KSK & ZSK key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide and the Verisign Information and Physical Security Policies. The activities performed in each Key Generation Ceremony are recorded, and such records are 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 XML from the CBO. Public-key information for the ZSKs comes to the data centers locked inside of the HSMs that are delivered by CBO personnel.

5.1.3. Public key parameters generation and quality checking

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.

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 TLD/GTLD zone KSK & ZSK private key will be used only for signing the relevant TLD/GTLD zones' RRsets or self-signing its own DNSKEY RR sets to provide proof of possession of private key.

Any resulting RRSIG record will not have a validity period longer than 15 days and will not extend more than 15 days into the future. The RRSIG produced by the ZSK is valid for 7 days and the RRSIG produced by the KSK is valid for 15 days.

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 the 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 & ZSK key pair generation and private key storage, Verisign uses hardware security modules 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 individuals to perform sensitive cryptographic operations. Verisign uses "Secret Sharing" to split the activation data needed to make use of an TLD/GTLD KSK & ZSK private key into separate parts called "Secret Shares" that 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 created and distributed for a particular hardware security module is required to activate a TLD/GTLD ZSK private key stored on the module. The threshold number of shares needed to sign a TLD/GTLD Zone File is 3.

It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational 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 TLD/GTLD KSK & 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 hardware cryptographic modules and associated key storage devices. Cryptographic modules used for private key storage meet the requirements of this DPS. Private keys are copied to backup hardware cryptographic modules in accordance with this DPS. Modules containing on-site backup copies of TLD/GTLD KSK and ZSK private keys are subject to the requirements of this DPS. Modules 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 on cryptographic module

Private keys held on hardware cryptographic modules 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 for any signing events after their supersession and will be zeroized after the HSMs are decommissioned.

5.2.7. Private key transfer into or from a cryptographic 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 modules in encrypted form.

5.2.8. Method of activating private key

The TLD/GTLD KSK and ZSK private key will be activated using a minimum of 3 MofN Secret Shares.

5.2.9. Method of deactivating private key

Verisign TLD/GTLD KSK and ZSK private keys are deactivated 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 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 ZSK and KSK public keys are backed up and archived as part of Verisign's routine backup procedures.

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 & ZSK will never be reused to sign a resource record.

5.4. Activation data

5.4.1. Activation data generation and installation

Activation data (Secret Shares) used to protect HSMs containing Verisign TLD/GTLD KSK and ZSK private keys is 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 KSK and ZSK private keys is transmitted directly from the Host IS platform 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.

Activation data for 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. After the record retention periods in section 5.2.6 lapse, Verisign will decommission activation data by overwriting and/or physical destruction.

5.5. Computer Security Controls

Verisign ensures that the systems maintaining key software and data files are Trustworthy Systems secure 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 its online signing functions using networks secured in accordance with the Verisign Information 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 application 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

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 and monitor the configuration of its systems. Verisign creates a hash of all software packages installed on production systems. This hash may be used to verify the integrity of such software for forensic purposes, although in practice host-based intrusion detection is used to alert when critical software packages are modified.

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.

Critical hardware components of the signer system (HSM) will be procured directly from the manufacturer and transported in tamper-evident bags to their destination in the secure facility. Any hardware will be decommissioned well before the specified life time 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 Records (NSEC3) 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 Records (NSEC) and creates signatures for all relevant records. The TLD/GTLD Zone is then distributed to the TLD/GTLD Server Operators.
The continuous TLD/GTLD Zone signing will be conducted automatically by the TLD/GTLD Zone Maintainer.

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 TLD/GTLD KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits.
The current TLD/GTLD ZSK key pair(s) is an RSA key pair, with a modulus size of 1024 bits.

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 RFC 5155 [RFC5155].

Option 2: Authenticated denial of existence will be provided through the use of NSEC 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.

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. Zone signing key roll-over

TLD/GTLD ZSK rollover is carried out quarterly automatically 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 these gatherings are pre-generated and signed at the same occasion with the projected signature inception and expiration time.

6.5. Key signing key roll-over

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.

6.6. Signature life-time and re-signing frequency

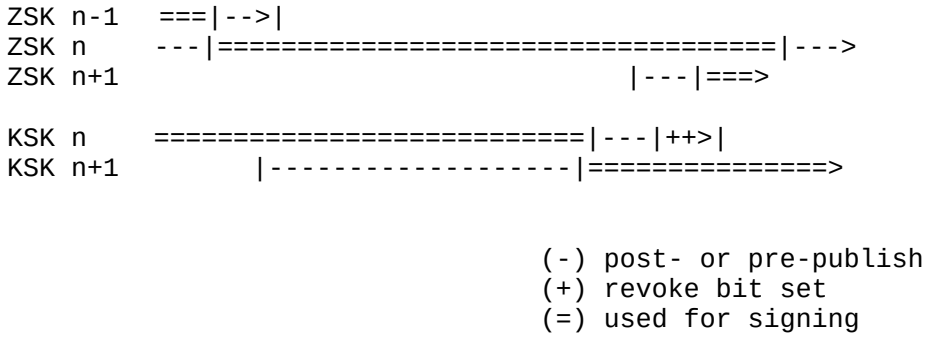
The signing practice of the TLD/GTLD Zone is divided into quarterly continuous time cycles of approximately 90 days. Time cycles begins at the following dates each year:

January 15th
April 15th
July 15th
October 15th

All DNSKEY records produced by the changes listed above are (1) known in advance and (2) signed in advance by the TLD/GTLD KSK. The collection of DNSKEY records for which Verisign pre-generates digital signatures consists of a 1-year period.

The time cycle will never be less than 90 days, except in emergency situations (where a key has been compromised) or if Verisign decides to begin using different key lengths.

A new ZSK is generated by the TLD/GTLD Zone Maintainer to be used for each new time cycle. Hence a TLD/GTLD ZSK roll-over is performed at the edge of every time cycle.



90 day cycle with ZSK and KSK roll over

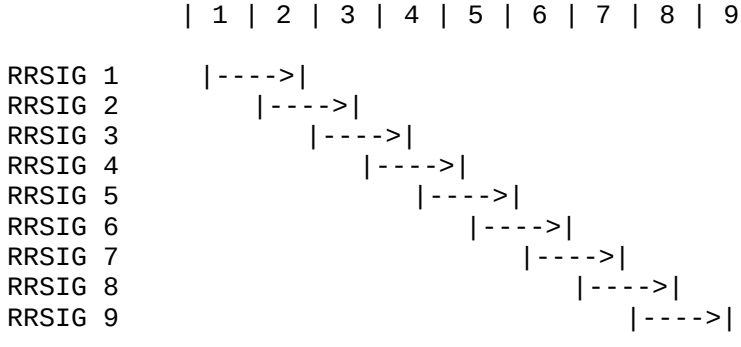
Figure 1

In the event of a ZSK roll-over, 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 7 days.

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



DNSKEY RRSIG's validity period within the cycle

Figure 2

6.7. Verification of zone signing key set

The KSK operator's system will verify the signature data is authentic by validating the public key data contained in the KSR.

6.8. Verification of resource records

The Extractor/Validator system verifies all resource record signatures prior to distribution. The integrity of the unsigned zone contents is also validated prior to distribution.

6.9. Resource records time-to-live

RRtype	TTL
DNSKey	24 hours
Delegation Signer (DS)	24 hours
RRSIG	same as the covered RR (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

Compliance 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 ZSK and KSK.

7.4. Topics covered by audit

The scope of Verisign's annual Compliance Audit includes all DNSSEC operations such as 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 with input from the auditor. 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 http://www.verisigninc.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 (Confidential/Private Information):

- 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
- Audit reports created by Verisign (to the extent such reports are maintained), and their respective auditors (whether internal or public)
- Contingency planning and disaster recovery plans
- 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, Key Revocation, 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, personally identifiable information in the course of providing TLD/GTLD services, such PII is treated as private in accordance with Verisign's Privacy Policy as set forth at http://www.verisigninc.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 services, Verisign acts as a data processor and not as a data controller, and any obligations that Verisign may have with respect to any personally identifiable information 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 http://www.verisigninc.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 DNSSEC Practice Statement for the TLD/GTLD Zone KSK and ZSK Operator. No other liability, implicit or explicit, is accepted.

8.6. Term and termination

8.6.1. Term

The 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.

8.6.3. 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 sixty (60) days followed by litigation in the federal or state court encompassing Fairfax County, Virginia.

8.6.4. Governing law

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

Appendix A. Table of acronyms and definitions

A.1. Acronyms

Table of Acronyms

Term	Definition
AD	Authenticated Data Flag
AICPA	American Institute of Certified Public Accountants
BIND	Berkley Internet Name Domain
CC	Common Criteria
CD	Checking Disabled
DNS	Domain Name System
DNSKEY	Domain Name System Key
DNSSEC	Domain Name System Security Extensions
DO	DNSSEC OK Flag
DPS	DNSSEC Practices Statement
DS	Delegation Signer
EAL	Evaluation Assurance Level (pursuant to the Common Criteria)
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
gTLD	Generic Top Level Domain
HSM	Hardware Security Module
ISO	International Organization for Standardization
KSKO	Key Signing Key Operator
NIST	National Institute of Standards and Technology
NS	Name Server
NSEC	NextSecure
NSEC3	NextSecure3
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RFC	Request for Comments
RRSIG	Resource Record Signature
SEP	Secure Entry Point
SHA	Secure Hash Algorithm
SOA	Start of Authority
SP	NIST Special Publication
TLD	Top Level Domain
TSIG	Transaction Signature
TTL	Time To Live
VERT	Verisign Emergency Response Team
VSIRT	Verisign Security Incident Response Team
ZSKO	Zone Signing Key Operator

A.2. Definitions

Definitions

Term	Definition
Chain of Trust	DNS keys, signatures and delegation signer records linked together forming a chain of signed data.
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 a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with standards that apply to it.
Confidential/Private Information	Information required to be kept confidential and private.
Delegation Signer (DS)	Delegation Signer (DS) is one of the resource records in the zone file indicating that the delegated zone is digitally signed. It also assures that the parent zone recognizes the indicated key for the delegated zone.
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 Generation Ceremony	A procedure whereby a key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or key sets are signed.
Key Signing Key (KSK)	A key that signs the key set.
Management Review	Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Offline HSM	HSMs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These HSMs do not directly sign the zone file
Online HSM	HSMs that sign the Zone file under the Zone Signing Key are maintained online so as to provide continuous signing services.
Parent Zone	The zone which is one level higher.
Policy Management Authority (PMA)	The organization within Verisign responsible for promulgating this policy.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a public key cryptographic system.
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 a private key or a portion of the activation data needed to operate a private key under a Secret Sharing arrangement.
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 Position	The positions within the DNSSEC operations that must be held by a Trusted Person.
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.
Repository	DNSSEC related information made accessible online.
Zone	A boundary of responsibility for each domain.
Zone Signing Key (ZSK)	A key that signs the COM Zone

Appendix B. History of Changes

History of Changes: Version 1.3

Section	Description
Cover page	Updated the version number, date, and copyright year
Table of Contents	Updated
1.1	Used auto bullet points rather than manual bullet points. Changed "- The Verisign Physical Security Policy - Sets forth security principles governing the DPS infrastructure - The Verisign Information and Physical Security Policies describe detailed requirements for Verisign concerning personnel, physical, telecommunications, and logical security. - The Key Ceremony Reference Guide - Presents detailed key management operational requirements" to • "The Verisign Physical Security Policy – Describes physical and personnel security requirements • The Verisign Information Security Policy – Describes telecommunications and logical security requirements • The Verisign Cryptographic Key Management Guide – Describes cryptographic key management security • The Verisign Key Ceremony Guide – Describes the procedures used to generate cryptographic keys"
1.3.5	Updated to use auto numbering rather than manual numbering
1.3.6	Updated to use auto numbering rather than manual numbering
1.3.7	Updated to use auto numbering rather than manual numbering
1.4.2	Changed "The DPS Practices Manager" to "The DNSSEC Practices Manager"
4.2.1	Used auto bullet points rather than manual bullet points.
4.2.3	Used auto bullet points rather than manual bullet points.
4.3.2	Used auto bullet points rather than manual bullet points.
4.3.3	Used auto bullet points rather than manual bullet points.
4.4.1	Used auto bullet points rather than manual bullet points.
4.5.4	Added ", the Verisign Cryptographic Key Management Security Guide and the Verisign Key Ceremony Guide" Used auto bullet points rather than manual bullet points.
5.7	Used auto bullet points rather than manual bullet points.
8.3.1	Used auto bullet points rather than manual bullet points.
8.6.2	Changed "as amended" to "is amended"