DNSSEC Practice Statement for the Verisign Managed DNS Service

Version: 1.7

Effective Date: December 21, 2018

Abstract

This document is the DNSSEC Practice Statement (DPS) for the Verisign Managed DNS (MDNS) Service. It states the practices and provisions that are employed in providing signing and zone distribution functions, such as issuing, managing, changing, and distributing Domain Name System (DNS) keys, for the Verisign MDNS Service.

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

Table of Contents

1 INTRODUCTION

This document is the DPS for the Verisign MDNS Service. It states the practices and provisions that are employed in providing signing and zone distribution functions, such as issuing, managing, changing and distributing DNS keys, for the Verisign MDNS 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 Verisign MDNS Service. More generally, this document will provide the governing policies and provisions as they relate to the management, security and technical specifications of the Verisign MDNS Service customer 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 will be made public as required.

This DPS is only one of a set of documents relevant to Verisign's management of the Verisign MDNS Service customer 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;
- 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 sensitive information and will not be publicly disclosed.

1.2 Document Name and Identification

DNSSEC Practice Statement for the Verisign Managed DNS Service

1.3 Community and Applicability

1.3.1 Verisign MDNS Service Manager

The Verisign MDNS Service manager is Verisign.

1.3.2 Verisign MDNS Service Administrator

The Verisign MDNS Service administrator is Verisign.

1.3.3 Verisign MDNS Service Maintainer

The Verisign MDNS Service maintainer is Verisign.

1.3.4 Verisign MDNS Service Server Operator

The Verisign MDNS Service operator is Verisign.

1.3.5 Verisign MDNS Service Key Wrapping Key Operator

Verisign, as the MDNS Service's Key Wrapping Key (KWK) operator, performs the function of generating the symmetric KWK. The KWK is used to encrypt the private portions of the key pairs for external storage, and to decrypt the private portions within the HSM for zone signing activities, including creating a valid DNSKEY resource record set (RRset).

1.3.6 Verisign MDNS Service Key Signing Key Operator

The Verisign MDNS Service's KSK operator is Verisign. The Verisign MDNS Service's KSK operator is responsible for:

1) generating and protecting the private component of the customer KSK,
2) securely importing key components from the Verisign MDNS Service operator,
3) authenticating and validating the public customer ZSK keyset,
4) securely signing each domain's keyset (i.e., all DNSKEY records) with that domain's protected private KSK,
5) securely exporting each domain's public key components,
6) securely transmitting each domain's DNSKEY RRset to the Verisign MDNS Service operator, and
7) issuing an emergency key rollover within a reasonable amount of time if any KSK associated with a zone is lost or suspected by Verisign to be compromised.

1.3.7 Verisign MDNS Service Zone Signing Key Operator

The Verisign MDNS Service's ZSK operator is Verisign. The Verisign MDNS Service's ZSK operator is responsible for:

1) generating and protecting the private component of the customer ZSK,

2) securely exporting and transmitting the public customer zone ZSK component to the Verisign MDNS Service KSK operator,
3) securely importing the signed customer zone DNSKEY RRset from the Verisign MDNS Service KSK operator,
4) signing the authoritative resource records for the customer domain, 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.

1.4 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

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. 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 Signed Zone

The Verisign MDNS Service publishes the customer's signed zone on Verisign name servers.

2.2 Repositories

Verisign publishes this DPS in the repository section of Verisign's web site at:
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. 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 publication of a signed DS record for that child zone in the parent zone. The DS record is a cryptographic shorthand representation, or hash, of the public portion of the child zone generated and controlled KSK. It establishes a chain of trust from the parent 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 as it only applies changes received from MDNS customers.

3.4 Registration of Delegation Signer Records

It is the customer's responsibility to publish their zone's DS record in the parent zone.

3.5 Removal of Delegation Signer Records

It is the customer's responsibility to remove their zone's DS record from the parent zone.

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 associated with the KWK and the private KSK and ZSK keys 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 the KWK 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 Verisign MDNS KWK.

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., HSM) 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 the Verisign MDNS Service KWK.

Designated third-party audit personnel may not participate in the multi-person control for the KWK.

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 Verisign MDNS Service 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 resource 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:

Verisign MDNS Service KWK life cycle management events, including:

- key generation, cloning, storage, recovery, archival, and destruction, and
- cryptographic device life cycle management events.

Verisign MDNS Service KWK 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 customer 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 a periodic basis. 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. Compromise of the KWK would compromise the KSKs and the ZSKs, and the emergency KWK rollover procedure will be enacted.

Verisign will follow its incident handling procedures set forth in the 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 key compromise or disaster recovery procedures will be implemented.

4.5.3 Entity Private Key Compromise Procedures

4.5.3.1 Key Signing Key or Zone Signing Key Compromise

Upon the suspected or confirmed compromise of the customer zone KSK or ZSK, 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 Key Wrapping Key Compromise

Upon the suspected or confirmed compromise of the KWK, 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,
- generation, encryption, and decryption of KSKs,
- generation, encryption, and decryption of ZSKs,
- signing of a zone file, and
- distribution of a signed zone file.

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. 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

Not applicable.

5 TECHNICAL SECURITY CONTROLS

5.1 Key Generation and Installation

5.1.1 Key Generation

The Verisign MDNS Service KWK generation is 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 the KWK and for the customer zone KSK and ZSK key generations meet the requirements of Federal Information Processing Standards (FIPS) 140-2 level 3.

The KWK is 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 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 also will include validating the size of the public exponent to be both resource-efficient and secure.

5.1.3 Key Usage Purposes

Any Verisign MDNS Service KSK or ZSK private key will be used only for signing the corresponding RRsets or self-signing its own DNSKEY RRsets to provide proof of possession of the private key.

Any resulting RRSIG record will have a validity period of 10-20 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 an authorized HSM; that is, the private component will not be exported from the HSM except in encrypted form for purposes of key archival. The private keys are encrypted by the HSM using the KWK within the HSM before export.

5.2.1 Cryptographic Module Standards and Controls

For Verisign MDNS Service KSK & ZSK key pair generation and signing, 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 KWK 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 the KWK 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 HSM 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 customer zone KSK and ZSK are not escrowed.

5.2.4 Private Key Backup

Verisign creates backup copies of MDNS Service customer zone KSK and ZSK private keys for routine recovery and disaster recovery purposes.

5.2.5 Private Key Unencrypted Only Within Cryptographic Module

Private keys may not leave the HSM without first being encrypted with the symmetric KWK. The private keys are stored in encrypted form in a transactional database.

5.2.6 Private Key Archival

The Verisign MDNS Service customer zone KSK and ZSK key pairs do not expire, but are retired when superseded. Superseded key pairs will not be used after their supersession. Decommissioned HSMs will be zeroized and/or physically destroyed.

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

Verisign generates the Verisign MDNS Service customer zone KSK and ZSK key pairs on the HSMs, in which the keys will be used, for zone signing purposes, and then exports them to a transactional database. All copies of private keys outside the HSM module are HSM encrypted.

5.2.8 Method of Activating Key Wrapping Key

The Verisign MDNS Service KWK will be set to an activated state using a minimum of three "Secret Shares".

5.2.9 Method of Deactivating Key Wrapping Key

The Verisign MDNS Service KWK is set to an inactive state upon system shutdown.

5.2.10 Method of Destroying Key Wrapping Key

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

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

Customer zone KSK and ZSK public keys are backed up and archived.

5.3.2 Key Usage Periods

The operational period of each Verisign MDNS Service customer zone KSK and ZSK ends upon its supersession. The superseded customer zone KSK and ZSK are never reused.

5.4 Activation Data

5.4.1 Activation Data Generation

Activation data (contained in "Secret Shares") used to activate HSMs containing the Verisign MDNS Service KWK 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 MDNS 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 KWK 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.

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.

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 Verisign MDNS Service maintainer inserts the customer domain keyset into the customer zone, adds the Next Secure (NSEC/NSEC3) records as appropriate, and creates signatures for all relevant records. The updated customer zone is hosted by the MDNS service.

The Verisign MDNS Service will re-sign the customer zone automatically.

6.1 Key Lengths, Key Types, and Algorithms

The symmetric KWK is required to be of sufficient length to ensure that any encrypted customer domain private key cannot be decrypted.

The current KWK is a 256 bit AES key.

Customer domain 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 customer zone KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits.
The current customer zone ZSK key pair(s) is an RSA key pair, with a modulus size of at least 1024 bits.

6.2 Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC or NSEC3 records as specified in Request for Comments (RFC) 4033-35 and RFC 5155.

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.

The MDNS Service customer zone KSK and ZSK signatures will be generated by encrypting SHA-256 hashes using RSA[RFC5702].

6.4 Key Signing Key Rollover and Schedule

There are no scheduled MDNS KSK rollovers, but Verisign will assess the need for MDNS KSK rollovers approximately once a year. In the event that a KSK rollover (either planned or emergency due to compromised key) is performed, MDNS will continue to publish the old KSK until Verisign has verified the new DS record has been added to the parent zone. The process will ensure chain of trust between zones is not

broken.

6.5 Zone Signing Key Rollover and Schedule

Customer zone ZSK rollovers are carried out every 90 days.

Period	Value	Description
Active	90 days	The number of days a key is used to sign a zone before rolling over to a new key.
Pre-publish	7 days	Before we begin to sign a zone with a key, we pre-publish the key in the zone for this period.
Post-publish	7 days	After the old key is rolled over, it is still published (though nothing is signed with it) in the zone for this period.
Emergency Rollover Post-publish	2 days	If a ZSK is believed to be compromised, an emergency rollover of the ZSK will result in the old key still being published in the zone for 2 days (to make sure caching resolvers don't break), but the zone is not signed with it.

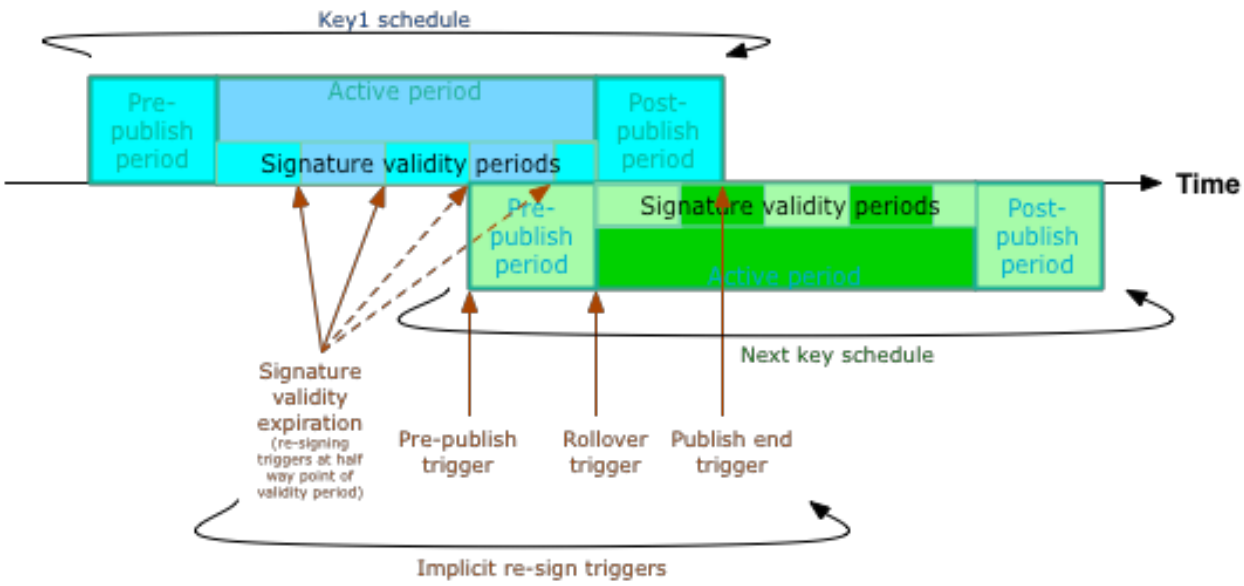
6.6 Key Wrapping Key Rollover

Neither the KWK nor its encryption products are exposed to the public; it is normally not rolled over. It may be rolled over in an emergency situation.

6.7 Signature Life-Time and Re-Signing Frequency

The below diagram depicts when a zone is resigned based on key schedule. The concept of active, pre-publish & post-publish periods shown in the diagram apply to both KSK & ZSK.

The schedule on top is for Key1, and the green schedule below is for the next key to be rolled over to, on a horizontal time line.

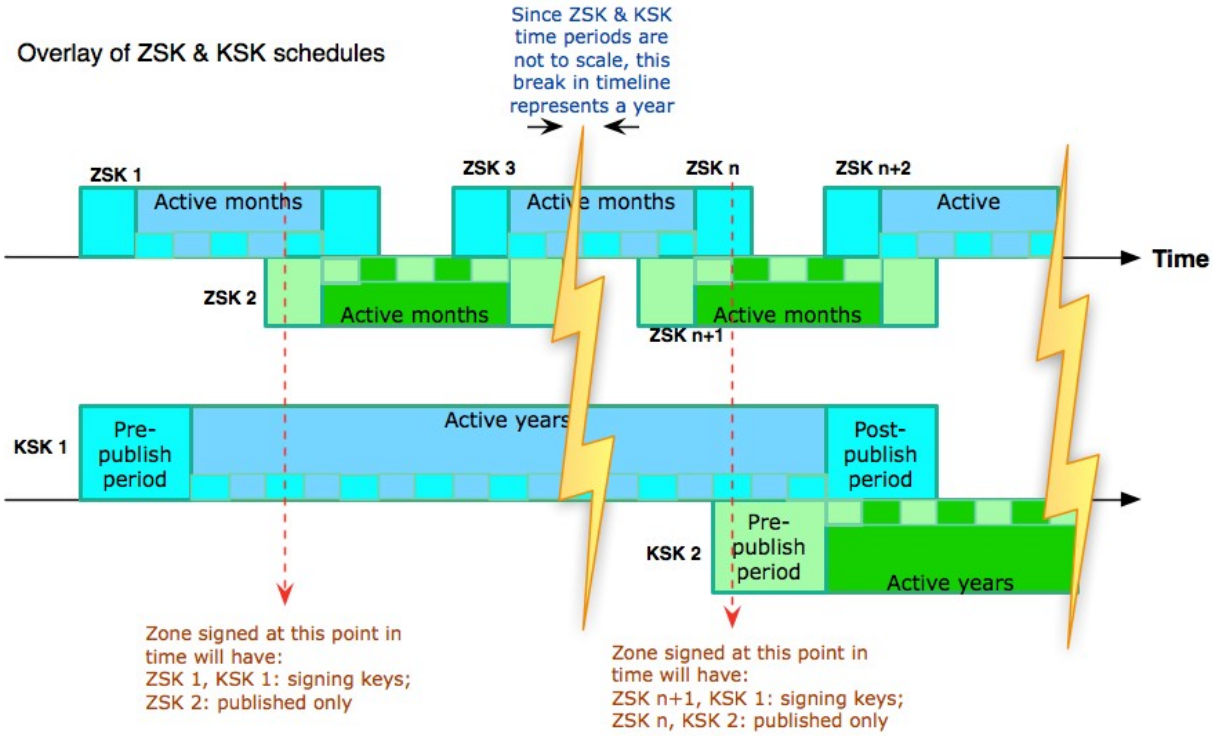


If an explicit sign request comes in (e.g., a zone update), then the system looks up the schedule for that instant in time, and signs with the keys that are in "Active Period". If a key is in pre or post publish period (see diagrams), at that instant, then that key is merely published in the signed zone.

If a signing request happens to come in at exactly the instant in time when a rollover is scheduled then only one of the keys will be used for signing and the other will be merely published.

The system also actively monitors and re-signs at times when there is no explicit request. This occurs when a key needs to pre-published, rolled over, at the half way of the "Signature Validity Period" (see in diagrams) of the RRSIGs in the zone (Since our Signature Validity Period is 14 days, this works out to an automatic re-sign, approx. 7 days after any sign activity), and at the end of the post-publish period.

The below diagram depicts both ZSK & KSK schedules together to provide a complete picture.



6.8 Verification of Resource Records

The extractor/validator system verifies all resource record signatures (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	1 hour
DS	24 hours by default; can be changed by customer
NSEC 3	Same as the minimum field in the zone SOA RR
RRSIG	Same as the covered RRset

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 MDNS signing services including the Verisign MDNS Service customer zone 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 to Verisign. Third-party auditors do not participate in the multi-person control for the KWK.

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, customer zone 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 customer zone 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.

8 MISCELLANEOUS

8.1 Fees

Verisign reserves the right to charge fees for the Verisign MDNS Service.

8.2 Governing Law

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

8.3 Term and Termination

8.3.1 Term

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

8.3.2 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

Acronym	Term
AES	Advanced Encryption Standard
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
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
KSK	Key Signing Key
MDNS	Managed Domain Name System
NSEC	Next Secure
NSEC3	Next Secure3
PII	Personal Identifiable Information
PMA	Policy Management Authority
RFC	Request for Comments
RRSIG	Resource Record Signature
SHA	Secure Hash Algorithm
SOA	Start of Authority
TTL	Time-To-Live
IRT	Verisign Incident Response Team
KWK	Key Wrapping Key
ZSK	Zone Signing Key

A.2 Terms

Term	Definition
Chain of Trust	DNS keys, signatures and delegation signer records linked together forming a chain of signed data.
Child Zone	A boundary of responsibility for a domain that exists one level higher than the referenced zone.
Compliance Audit	A periodic audit that Verisign undergoes to determine its conformance with standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private.
Cryptographic Key Generation Ceremony	A procedure whereby a KWK is generated.
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	Resource Record that stores the public version of a KSK or ZSK.
Key Signing Key (KSK)	A key that signs the DNSKEY RRset.
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, and/or to provide the KWK for disaster recovery purposes.
Online HSM	An HSM that signs the zone file using the ZSK and is maintained online so as to provide continuous signing services.
Parent Zone	A boundary of responsibility for a domain with at least one subdomain.
Policy Management Authority (PMA)	The organization within Verisign responsible for promulgating this policy.
Repository	A location on the Verisign web site where DNSSEC related information is made accessible online.
Resource Record Signature (RRSIG)	Signature of a DNSSEC-secured record set.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Supersede	A key is superseded when it stops being published in its respective zone.
Secret Share	The activation data needed to utilize the key wrapping key under a Secret Sharing arrangement.
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.
Key Wrapping Key (KWK)	A key that encrypts and decrypts keys moving in and out of an HSM.
Zone	A boundary of responsibility for each domain.
Zone Signing Key (ZSK)	A key that signs the domains covered by the Verisign MDNS Service.

Appendix B Changes from Previous Version

Changes from Previous Version: 1.5

Section	Description
Cover page	Changed Version to 1.7 Changed Effective Date to TBD Changed ”2017” to “2018”
Entire Document	Added quotes from all instances of Secret Shares.
1.1	Remove colon from "Other documents include: " Changed "The Verisign Information Security Policy - Describes information security requirements;" to "Verisign Information Security Documentation – Describes information security requirements;" Changed "Verisign sensitive information" to "Verisign confidential information"
1.3.6	Added “by Verisign”
1.3.7	Added “by Verisign”
4.1	Changed “sensitive information” to “confidential information”
4.1.5	Changed “precautions” to “measures”
4.2.1	Added “(CBO)” Removed “may”
4.2.2	Changed "device" to "cryptographic hardware device" Changed “i.e.” to “e.g.” Changed “Trusted Personnel” to “Trusted Persons”
4.2.3	Changed “Trusted Persons” to “a Trusted Person” Changed “in person” to “in-person” Changed “Trusted Persons” to “Trusted Person”
4.3.1	Removed comma after citizenship
4.3.2	Changed “candidates” to “ a candidate” Changed “Trusted Persons” to “Trusted Person”
4.3.4	Removed “their”
4.3.8	Changed “employees” to “personnel”
4.4.2	Changed “periodically” to “at least once annually”
4.4.5	Changed “will be” to “are”
4.4.6	Changed “paper based” to “paper-based”
4.4.8	Changed “security requirements” to “Security Documentation”
4.5.1	Changed “information security requirements” to “Information Security Documentation”
4.5.2	Removed comma
4.5.3.1	Removed “V” from “VIRT”; Changed “Cryptographic Business Operations” to “CBO”
4.5.3.2	Removed “V” from “VIRT”; Changed “Cryptographic Business Operations” to “CBO”
4.5.4	Added “secure”; Removed "Verisign plans are regularly tested, validated, and updated so that Verisign systems, services and key business functions can be operational in the event of any incident or disaster."
5.2.2	Added (M) and (N) for clarification of shares in 2nd paragraph
5.7	Added “Network Time Protocol (NTP)” Changed “paper based” to “paper-based” Changed “signatures” to “signature”
5.8.3	Changed “bags” to “packaging”; changed “well before the” to “prior to its”
6.1	Added “at least” to ZSK key pair modulus size

7.3	Changed “Third party” to “Third-party”
A.1	Added “CBO - Cryptographic Business Operations” to Appendix A; Changed “VIRT” to “IRT”
A.2	Offline HSM - Changed HSM to singular form; Online HSM - changed HSM to singular form