Verisign, Inc.

System and Organization Controls 3 (SOC3®)

Report on Verisign, Inc.'s Controls Over the Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System, Related to the Managed DNSSEC System, Relevant to Security, Availability, and Processing Integrity Throughout the Period April 1, 2019 to December 31, 2019

Prepared in Accordance with AT-C 205 pursuant to

TSP Section 100, *2017 Trust Services Criteria*

for Security, Availability, Processing Integrity, Confidentiality, and Privacy

***(AICPA, Trust Services Criteria*)**

Contents

I. Report of Independent Service Auditors

Report of Independent Service Auditors

To the Management of Verisign, Inc.

Scope

We have examined Verisign, Inc.'s accompanying assertion titled "Management of Verisign, Inc.'s Assertion" ("assertion") that the controls within Verisign, Inc.'s Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the Managed DNSSEC system, ("system") were effective throughout the period April 1, 2019 to December 31, 2019, to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity ("applicable trust services criteria") set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Criteria*).

Service Organization's Responsibilities

Verisign, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements were achieved. Verisign, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Verisign, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Verisign, Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Verisign, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Verisign, Inc.'s Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the Managed DNSSEC system, were effective throughout the period April 1, 2019 to December 31, 2019, to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP
May 1, 2020

II. Management of Verisign, Inc.'s Assertion

Management of Verisign, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Verisign, Inc.'s Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the Managed DNSSEC system, ("system") throughout the period April 1, 2019 to December 31, 2019, to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements relevant to security, availability, and processing integrity were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2019 to December 31, 2019, to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity ("applicable trust services criteria") set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).* Verisign, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2019 to December 31, 2019, to provide reasonable assurance that Verisign, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Verisign, Inc.
May 1, 2020

Attachment A

Verisign, Inc.'s Description of the Boundaries of Its Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System, Related to the Managed DNSSEC System

Services Provided

Verisign, Inc. (Verisign) is a provider of Internet infrastructure services for the networked world. Verisign helps companies and consumers all over the world to engage in trusted communications and commerce and employs approximately 1,000 people, primarily in the northern Virginia region, with sales and support operations provided in several other small regional offices. Verisign's core businesses consist of the following:

- The Naming Services business unit is responsible for services associated with the .net, .com, and other Top Level Domain (TLD) contracts, and for governing the Domain Name Systems Security Extensions (DNSSEC) systems and supporting services; and
- The Verisign Security Services (VSS) business unit provides Denial of Service (DoS) attack protection and managed DNS services. The DoS protection services, commercially branded as the Verisign Distributed DOS Protection Service (VDPS), leverages the high capacity of the DNS constellation systems to filter attack traffic being sent to a customer, which it then routes to its intended destination. The Managed DNS Services (MDNS) provides DNS resolution management for commercial customers with optional DNSSEC extensions.

The Verisign CBO and DNSSEC system, related to the Managed DNSSEC system and surrounding infrastructure (collectively referred to as "the system") is the subject of the SOC3℠ attestation examination conducted in accordance with the American Institute of Certified Public Accountants (AICPA) Trust Services guidelines and includes the following elements:

- *Infrastructure*. The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that Verisign uses to provide the services
- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the application in use are mobile applications or desktop or laptop applications
- *People*. The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers)
- *Data*. The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system
- *Procedures*. The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared

DNSSEC Signing System for Managed DNS

The Internet is an increasingly critical infrastructure for the effective functioning of government, economy, society, and national security. Verisign offers DNSSEC as an option to Managed DNS customers through the MDNS Signing service. Verisign signs the entire zone file for zones managed through the Managed DNS service.

DNSSEC is a set of Internet Engineering Task Force (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 has 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 root zone.

Zone File Signing

Verisign's Managed DNS signing servers sign the zone file on a periodic basis, update the DS Records on a regular basis, and publish the updates through the DNS Infrastructure.

Verisign is the Key Wrapping Key (KWK), Key Signing Key (KSK), and Zone Signing Key (ZSK) operator for the Managed DNS Signing Services. Verisign's Managed DNS Signing Services KWKs are generated during planned key ceremonies in accordance with documented policies by multiple trained and trusted individuals using processes that provide for the security and integrity of the generated keys.

Verisign generates the Managed DNS Signing KWKs, KSKs and ZSKs within Federal Information Processing Standard Publication (FIPS) 140-2 Level 3 cryptographic hardware. Significant key generation ceremony activities are recorded, dated and signed by all individuals involved. Verisign creates backup copies of the KWK, KSK and ZSK key pairs for routine recovery and disaster recovery purposes.

Verisign has created and published the Verisign DNSSEC Practice Statement (DPS) for Managed DNS Signing Services. It states the practices and provisions that Verisign employs in providing Verisign Managed DNS Signing Services.

Verisign publishes the DPS in the Repository section of Verisign's web site.

Infrastructure

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. 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.

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 activities, i.e., any activity related to the lifecycle of the KWK, KSKs and ZSKs, occur within restrictive physical tiers.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of Hardware Security Modules (HSM) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. More restricted areas require the presence of two authorized individuals for access. Online HSMs are protected through the use of locked cabinets. Offline HSMs are protected through the use of tamper- evident bags and 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 or containers housing key materials are logged.

Physical access is logged and recorded by Closed Circuit Television (CCTV). Authorized personnel are required to escort visitors or employees without authorization to enter the restricted tiers.

Computer Security Controls

Verisign ensures that the systems maintaining key software and data files are secure from unauthorized access. In addition, Verisign limits access to production servers to those individuals with a valid business reason for such access. Passwords meeting Verisign's password policies for complexity and duration are used to restrict access to systems. Production servers are separated from the corporate network by jump hosts that require authentication before access is granted to the production network. Systems used to generate cryptographic keys are physically air gapped from networks. Monitoring and logging is performed for online servers, with notifications generated when unexpected conditions occur.

Cryptographic module standards and controls

HSMs that are validated at FIPS 140-2 Level 3 are used for MDNS key generation. The KWK is stored in an HSM and the KSK and ZSK private keys are encrypted with the KWK and stored in a database. All cryptographic functions involving the private component of the KWK, KSK, and ZSK are performed within the HSM. Verisign generates the KWK key pair on the HSM in which the keys will be used, which is then copied to multiple HSMs for redundancy and recovery purposes. When KWKs are transported between HSMs, such keys are transported in encrypted form during a planned key ceremony. KSK and ZSK key pairs

are generated on the HSMs in which the keys will be used and are exported to a database after they are encrypted using the KWK.

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 networks. Network segmentation restricts network access to authorized communications supporting defined application processes. Verisign uses routers and/or firewalls to protect the production network from internal and external intrusion and limits the network access to production systems related to key signing activities. Monitoring, logging, and intrusion protection systems are used to determine the health and security of the networks, with notifications generated when unexpected conditions occur.

Time stamping

DNSSEC signing system clocks are synchronized using an authoritative time source for accurate recording of event times for the following (including but not limited to):

- Electronic audit log records; and
- DNSSEC signatures inception and expiration times.

Software

Verisign utilizes commercial and custom developed software to deliver Managed DNS Signing Services. The Managed DNS Signing Services applications are developed and implemented by Verisign in accordance with Verisign systems development and change management standards. All development, maintenance, and change requests are formally tracked and documented.

Verisign software deployed on production systems can be traced to version control repositories. Verisign has mechanisms and policies in place to control and monitor the configuration of its systems.

Updates critical to the security and operations of the signer system are applied after formal testing and approval.

People

Trusted roles

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

- Generation and protection of the private component of the Managed DNS Signing Services KWK, KSK, and ZSK;
- Export or import of any public components; and
- Generation and signing of zone file data.

Trusted roles include, but are not limited to:

- Naming Provisioning and Resolution Operations personnel;
- Cryptographic Business Operations personnel;
- Security personnel;
- System administration personnel;
- Designated engineering personnel; and
- Executives that are designated to manage infrastructural trustworthiness.

Number of persons required per task
Verisign has established, maintains, and enforces 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 physical access to and management of cryptographic hardware, HSMs, and associated key material require multiple Trusted Persons. Other critical operations such as Key Destruction require the participation of at least two Trusted Persons.

Identification and authentication for each role
Employee status as a Trusted Person is obtained through the successful completion of enhanced background verification in accordance with Verisign's background investigations policy and is granted when employees present themselves before Human Resource or Security Personnel in order to perform a visual identity confirmation using government issued identification documents.

Procedures
Procedures related to the Verisign Managed DNS Signing Services System are included, but are not limited to, the following topics:

- Policy management including management of the Verisign DPS for Managed DNS Signing Services;
- Operations management including incident handling, configuration management, change management, patch management, compromise response planning, disaster recovery planning, backup operations and systems monitoring;
- Key management operations including key generation, key storage, key archival, key destruction and key usage;
- Physical security and environmental management including physical access controls, tiered zone access management, physical intrusion detection, physical activity logging and maintaining a stable environment for data center operations; and
- Personnel management including maintaining the personnel component of business continuity, assessing the integrity and skills of employees and disciplining employees.

Data
The Verisign Managed DNS Signing Services System data consists of the following:

- Managed DNS Signing Services KWK and associated cryptographic activation materials used to protect the KWK;
- Managed DNS Signing Services KSKs, associated cryptographic activation materials and database used to protect the KSKs;
- Managed DNS Signing Services ZSKs, associated cryptographic activation materials and database used to protect the ZSKs;
- Managed DNS Signing Services Signed Keysets;
- Managed DNS Signing Services Zone Files;
- Delegation Signer (DS) Resource Records; and
- System audit trail records including, but not limited to, logs of the significant events related to ZSK and KSK key life cycle management, ZSK and KSK signing and management, and system security.

Verisign performs routine backups of critical system data, audit log data, and other sensitive information. All media containing production software and data, audit, archive, or 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).

Key Management

Key Wrapping Key (KWK) Operator

Verisign is the KWK operator for the Managed DNS Signing Services and is responsible for generating and storing the KWK. Specifically, as KWK operator, Verisign is responsible for:

- Generating and protecting the Managed DNS Signing KWK;
- Securely encrypting the Managed DNS Signing ZSK and KSK keysets (i.e., all Domain Name System Key (DNSKEY) records);
- Securely decrypting the Managed DNS Signing Services ZSK and KSK keysets; and
- Issuing an emergency key roll-over within reasonable time if any KWK associated with the system is lost, compromised, or suspected to be compromised.

Key Signing Key (KSK) Operator

Verisign is the KSK operator for Managed DNS Signing and is responsible for generating the respective zones' KSKs, signing the zone keysets, storing the private keys, and distributing the public portion of the Key Signing Keys to the parent zone. Specifically, as Key Signing Key operator, Verisign is responsible for:

- Generating and protecting the private components of the Managed DNS Signing Services zones' KSKs;
- Securely importing public key components of the Managed DNS Signing zones' ZSKs;
- Authenticating and validating the public Managed DNS Signing zones' ZSK keysets;
- Securely signing the Managed DNS Signing zones' ZSK and KSK keysets (i.e., all DNSKEY records);
- Securely transmitting the respective signed Managed DNS Signing zones' DNSKEY Resource-Record Sets to the Managed DNS Signing ZSK operator;
- Securely exporting the Managed DNSSEC zones' KSK public key components;
- Creating a DS record from the KSK public key and submitting it back to the zone operator for insertion into the zone's parent zone; and
- Issuing an emergency key roll-over within reasonable time if any KSK associated with the zone is lost, compromised, or suspected to be compromised.

Zone Signing Key (ZSK) Operator

Verisign is also the ZSK operator for the Managed DNS Signing and is responsible for generating the respective Zones' ZSKs, signing the Zone Files, storing the private keys, and distributing the public portion of the Zone Signing Keys to the Key Signing Key Operator for signing. Specifically, as Zone Signing Key operator, Verisign is responsible for:

- Generating and protecting the private components of the Managed DNS Signing zones' ZSKs;
- Securely exporting and transmitting the public Managed DNS Signing zones' ZSK components to the KSK Operator;
- Securely importing the signed Managed DNS Signing zones' DNSKEY Resource Record Sets;
- Signing the Managed DNS Signing zone's authoritative resource records omitting the DNSKEY resource record; and
- Issuing an emergency key roll-over within a reasonable amount of time if any ZSK associated with the zones is lost, compromised, or suspected to be compromised.

Key Generation, Storage and Usage

The Verisign Managed DNS Signing Services KWK, ZSK, and KSK key pair generation is performed by trusted individuals using pre-planned key generation ceremonies. HSMs used for KWK, ZSK and KSK key pair generation are validated at FIPS 140-2 level 3. KWK, KSK, and ZSK private keys do not expire; when they are superseded, key pairs are securely archived in the HSMs and are never re-activated. Verisign KWK keys are stored within hardware cryptographic modules and are not exposed in plain-text outside of the HSM. The KSK and ZSK private keys are encrypted by the KWK and stored within a database, and are never exposed in plain-text outside of the HSM. KSK and ZSK public keys are backed up and archived.

The KWK operational period ends when it is superseded, and the key is then not re-used to encrypt KSK and ZSK key pairs. The operational period of a ZSK ends when it is superseded, and is then not re-used to sign a Resource Record (RR) while archived. The operational period of the KSKs ends when it is superseded when the zone owner requests a KSK rollover, and the KSK is not re-used to sign a Key Signing Request (KSR) when archived.

Key pairs are of sufficient length to prevent the determination of the private key using crypto-analysis. The current KSK key pairs are an RSA key pair with a modulus size of 2048 bits, and the current ZSK key pair(s) is an RSA key pair with a modulus size of 1024 bits. The KSK and ZSK signatures are generated by encrypting SHA-256 hashes of the public key using the private key.

Key rollover is performed quarterly in an automated process and the ZSK key signing process using the zone's KSK is conducted automatically every three months.

Attachment B

Principal Service Commitments and System Requirements

Attachment B

Principal Service Commitments and System Requirements

Verisign designs its processes and procedures related to Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the Managed DNSSEC system, to meet its objectives for its DNSSEC Services. Those objectives are based on Verisign's contractual service level commitments, applicable laws and regulations, and the financial, operational, and compliance requirements that Verisign has established for the services.

Security, availability, and processing integrity commitments are documented and communicated in Service Level Agreements (SLAs) and other publicly available applicable Verisign agreements, as well as in the description of the service offerings provided through Verisign's publicly available website.

Verisign has created and published the Verisign DNSSEC Practice Statement (DPS) for Managed DNSSEC. The DPS states the practices and provisions that Verisign employs in providing Verisign DNSSEC Signing Services for the Managed DNSSEC services.

Verisign establishes operational requirements that support the achievement of security, availability, and processing integrity commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Verisign's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the DNSSEC Services.