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 DNSSEC Root Zone Signing system, Relevant to Security, Availability, and Processing Integrity Throughout the Period January 1, 2017 to December 31, 2017

Prepared in Accordance with AT-C 205 pursuant to
TSP Section 100A, *Trust Services Principles and Criteria*
for Security, Availability, Processing Integrity, Confidentiality,
***and Privacy* (AICPA, *Trust Services Principles and Criteria, issued March 2016*)**

Contents

I. Report of Independent Accountants

pwc

Report of Independent Accountants

To the Management of Verisign, Inc.:

We have examined the accompanying management assertion of Verisign, Inc. titled "Management of Verisign, Inc.'s Assertion" ("assertion") that Verisign, Inc. maintained effective controls over the Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the DNSSEC Root Zone Signing system, ("system") that were suitably designed and operating effectively throughout the period January 1, 2017 to December 31, 2017 to provide reasonable assurance that Verisign, Inc.'s commitments and system requirements were achieved based on the criteria relevant to the security, availability, and processing integrity principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Principles and Criteria, issued March 2016*) ("applicable trust services criteria") and included as Attachment A. Verisign, Inc. management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

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 the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of Verisign, Inc.'s relevant controls over the security, availability, and processing integrity of the Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the DNSSEC Root Zone Signing system, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become ineffective.

In our opinion, management's assertion referred to above is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP
March 30, 2018

II. Management of Verisign, Inc.'s Assertion

Management of Verisign, Inc.'s Assertion

Based on our evaluation, we confirm to the best of our knowledge and belief that Verisign, Inc. maintained effective controls over the Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) system, related to the DNSSEC Root Zone Signing system, ("system") that were suitably designed and operating effectively throughout the period January 1, 2017 to December 31, 2017 to provide reasonable assurance that Verisign, Inc.'s commitments and system requirements were achieved based on the criteria relevant to the security, availability, and processing integrity principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)* ("applicable trust services criteria") and included as Attachment A. Our attached description of the system identifies the aspects of the system covered by our assertion.

Verisign, Inc.
March 30, 2018

III. Verisign, Inc.'s System Description

Verisign, Inc. Overview

Verisign, Inc. (Verisign) is a trusted 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 DDOS 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 DNSSEC Root Zone Signing 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 physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Procedures*. The automated and manual procedures.
- *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

DNSSEC for Root Zone

Verisign is acting as the Root Zone Maintainer and supports DNSSEC as a way to increase trust in the Internet. In July 2010, Verisign, working with the Internet Assigned Numbers Authority (IANA) and the U.S. Department of Commerce (DoC), completed deployment of DNSSEC in the Root Zone, the starting point of the DNS hierarchy. In the capacity of the Root Zone Signing Key Operator, Verisign is responsible to perform the function of generating the Root Zone's Zone Signing Key (ZSK) and signing the Root Zone File using the ZSK. Specifically, as Root Zone ZSK (RZ ZSK) operator, Verisign is responsible for:

- Generating and protecting the private component of the RZ ZSK;
- Securely exporting and transmitting the public RZ ZSK component to the RZ Key Signing Key (KSK) Operator;
- Securely importing the signed RZ ZSK keyset from the RZ KSK operator;
- Signing the Root Zone's resource records; and
- Issuing emergency key roll-over within a reasonable amount of time if any private key associated with the zone is lost, compromised, or suspected to be compromised.

The RZ ZSK key pair generation is performed in 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 RZ ZSK key pairs within Federal Information Processing Standard Publication (FIPS) 140-2 Level 4 certified secure cryptographic hardware security modules. The activities performed during each key generation ceremony are recorded, dated and signed by all individuals involved. Verisign creates backup copies of RZ ZSK private keys for routine recovery and disaster recovery purposes.

Verisign has created and published the Verisign DNSSEC Practice Statement (DPS) as the RZ ZSK Operator. The DPS states the practices and provisions that Verisign employs in providing Root Zone Signing and Zone distribution services that include, but are not limited to, issuing, managing, changing and distributing DNS keys. 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 RZ ZSK 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 RZ ZSK, occur within very restrictive physical tiers.

The physical security system includes protection for 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). Unescorted personnel, including visitors or employees without specific authorization, are not allowed into such secured areas.

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 bastion 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 4 are used for RZ ZSK key pair generation and RZ ZSK private key storage. All cryptographic functions involving the private component of the ZSK are performed within the HSM. Verisign generates RZ ZSK key pairs on a single HSM which are then copied to multiple HSMs for redundancy and recovery purposes. When key pairs are copied to another HSM, such key pairs are transported between modules in encrypted form and are performed during a planned key ceremony.

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 limit 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 DNSSEC Root Zone Signing Services. The DNSSEC Root Zone Signing 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 RZ 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 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 physical access to and management of cryptographic hardware, HSMs, and associated key material require multiple Trusted Persons. Other critical operations such as the signing of Zone File 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.

Relying Parties
A Relying Party is the entity relying on DNSSEC, such as security-aware validating resolvers and other applications performing validation of DNSSEC signatures. The relying party must properly configure and update the Trust Anchor as appropriate.

Procedures
Procedures related to the RZ ZSK system include, but are not limited to, the following topics:

- Policy management including management of the Verisign DPS and information security policy as the RZ ZSK Operator;
- 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 DNSSEC Root Zone Signing System data consists of the following:

- RZ ZSK and associated cryptographic activation materials used to protect the RZ ZSK;
- Root Zone Signed Keyset;
- Root Zone File;
- Delegation Signer (DS) Resource Records; and
- System audit trail records including, but not limited to, logs of the significant events related to RZ ZSK key life cycle management, RZ ZSK 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
The Verisign DNSSEC RZ ZSK key pair generation is performed by trusted individuals using a pre-planned Key Generation Ceremony. Hardware Security Modules (HSM) used for key pair generation are validated at FIPS 140-2 level 4. Root Zone private keys do not expire; when they are superseded, key pairs are securely archived in the HSMs and are never re-activated. Verisign private keys are stored within hardware cryptographic modules and are not exposed in plain-text outside of the HSM. RZ ZSK public keys are backed up and archived.

The operational period of a RZ ZSK ends when it is superseded, and the key is not re-used to sign a Resource Record (RR) while archived. Key pairs are of sufficient length to prevent the determination of the private key using crypto-analysis. The current RZ ZSK key pair(s) is an RSA key pair with a modulus size of at least 1024 bits. The RZ ZSK signatures are generated by encrypting the 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 is performed with the RZ KSK operator every three months. The RZ KSK operator function is currently performed by the IANA function of The Internet Corporation for Assigned Names and Numbers (ICANN).

Attachment A

Attachment A

Criteria Relevant to the Security, Availability and Processing Integrity Principles

Ref	Criteria
CC1.0	**Common Criteria Related to Organization and Management**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to *Security, Availability, and Processing Integrity.*
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting *Security, Availability, and Processing Integrity* and provides resources necessary for personnel to fulfill their responsibilities.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC2.0	**Common Criteria Related to Communications**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's *Security, Availability, and Processing Integrity* commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the *Security, Availability, and Processing Integrity* of the system, is provided to personnel to carry out their responsibilities.
CC2.5	Internal and external users have been provided with information on how to report *Security, Availability, and Processing Integrity* failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to *Security, Availability, and Processing Integrity* are communicated to those users in a timely manner.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**
CC3.1	The entity (1) identifies potential threats that could impair system *Security, Availability, and Processing Integrity* commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies

Ref	Criteria
	for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.
CC4.0	**Common Criteria Related to Monitoring of Controls**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC5.6	Logical access security measures have been implemented to protect against *Security, Availability, and Processing Integrity* threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.

Ref	Criteria
CC6.0	**Common Criteria Related to System Operations**
CC6.1	Vulnerabilities of system components to *Security, Availability, and Processing Integrity* breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC6.2	*Security, Availability, and Processing Integrity* incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
CC7.0	**Common Criteria Related to Change Management**
CC7.1	The entity's commitments and system requirements, as they relate to *Security, Availability, and Processing Integrity*, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to *Security, Availability, and Processing Integrity*.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's *Security, Availability, and Processing Integrity* commitments and system requirements.
Additional Criteria for Availability	
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.
Additional Criteria for Processing Integrity	
PI1.1	Procedures exist to prevent, or detect and correct, processing errors to meet the entity's processing integrity commitments and system requirements.
PI1.2	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
PI1.3	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.
PI1.4	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.
PI1.5	System output is complete, accurate, distributed, and retained to meet the entity's processing integrity commitments and system requirements.
PI1.6	Modification of data, other than routine transaction processing, is authorized and processed to meet with the entity's processing integrity commitments and system requirements.