VERISIGN, INC.

Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System related to the DNSSEC TLD/GTLD Zone Signing System

System and Organization Controls (SOC) for Service Organizations:
Trust Services Criteria for General Use Report (SOC 3)
for the period of January 1, 2024 to December 31, 2024

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

GRANT THORNTON LLP
1415 Vantage Park Drive, Suite 500
Charlotte, NC 28203

D +1 704 632 3500
F +1 704 334 7701

I. Report of Independent Service Auditors

Board of Directors and Management
Verisign, Inc.

Scope
We have examined Verisign, Inc.'s ("Verisign") accompanying assertion titled "*Verisign Inc.'s Assertion"* ("assertion") that the controls within Verisign's Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System related to the DNSSEC TLD/GTLD Zone Signing System ("system") were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that Verisign'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 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's service commitments and system requirements were achieved. Verisign has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Verisign 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's service commitments and system requirements based on the applicable trust services criteria; and
- performing procedures to obtain evidence about whether controls within the system were effective to achieve Verisign'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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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's Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System related to the DNSSEC TLD/GTLD Zone Signing System were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that Verisign's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Grant Thornton LLP

Charlotte, North Carolina
March 14, 2025

II. Verisign, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Verisign, Inc.’s (“Verisign”) Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System related to the DNSSEC TLD/GTLD Zone Signing System (“system”) throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that Verisign’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 January 1, 2024 to December 31, 2024, to provide reasonable assurance that Verisign’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’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 January 1, 2024 to December 31, 2024, to provide reasonable assurance that Verisign’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A – Verisign Inc.'s Description of the Boundaries of its System

A. Overview of 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 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 business, the Naming Services business unit, is responsible for services associated with the .net, .com, and other Top Level Domain (TLD) contracts and Generic Top Level Domain (GTLD) and for governing the Domain Name Systems Security Extensions (DNSSEC) systems and supporting services.

The Verisign CBO and DNSSEC System related to the DNSSEC TLD/GTLD Zone Signing System and surrounding infrastructure (collectively referred to as "the system") 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 TLD/GTLD Zones

The Internet is an increasingly critical infrastructure for the effective functioning of the government, the economy, society, and national security. Verisign offers DNSSEC as an option for domain registrants under the TLD/GTLD Zones. Verisign signs Delegation Signer (DS) Records in TLD/GTLD zones that have opted-in for signing. Verisign's DNSSEC signing servers sign updates to DS Records on a regular basis and publish the updates through the DNS Infrastructure.

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 validation is performed by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating at the root zone.

Verisign is the Key Signing Key (KSK) operator for the TLD/GTLD Zones and is responsible for generating the respective zone's KSK, for signing the zone keyset, for storing the private keys, and for distributing the public portion of the KSK to the parent zone. Specifically, as the KSK operator, Verisign is responsible for:

- Generating and protecting the private components of the TLD/GTLD KSK;
- Securely importing public key components of the TLD/GTLD Zone Signing Key (ZSK);

- Authenticating and validating the public TLD/GTLD ZSK keys;
- Securely signing the TLD/GTLD apex keyset (i.e., all Domain Name System Key (DNSKEY) records);
- Securely transmitting the respective signed TLD/GTLD DNSKEY Resource-Record Set to the TLD/GTLD ZSK operator;
- Securely exporting the TLD/GTLD KSK public key components;
- Creating a DS record from the KSK public key and preparing it for the TLD/GTLD registry of record who will submit this to Internet Assigned Numbers Authority (IANA) for insertion into the root 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.

Verisign is also the ZSK operator for the TLD/GTLD Zones and is responsible for generating the respective zone's ZSK, signing the zone file, for storing the private keys, and for distributing the public portion of the ZSK to the KSK Operator for signing. Specifically, as ZSK operator, Verisign is responsible for:

- Generating and protecting the private component of the TLD/GTLD ZSK;
- Securely exporting and transmitting the public TLD/GTLD ZSK component to the KSK Operator;
- Securely importing the signed TLD/GTLD DNSKEY Resource Record Set from the TLD/GTLD KSK Operator;
- Signing the TLD/GTLD 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 zone is lost, compromised, or suspected to be compromised.

TLD/GTLD Zone KSK and ZSK pairs are generated by multiple trained and trusted individuals using processes that provide for the security and integrity of the generated keys during planned key ceremonies in accordance with documented policies. Verisign generates TLD/GTLD KSK and ZSK key pairs within Federal Information Processing Standard Publication (FIPS) 140-2 Level 3 cryptographic hardware. Significant key generation ceremony activities are recorded, dated, and signed by the key individuals involved. Verisign creates backup copies of the KSK and ZSK key pairs for routine recovery and disaster recovery purposes.

Verisign has created and published the Verisign DNSSEC Practice Statement (DPS) for the TLD/GTLD zones. The DPS states the practices and provisions that Verisign employs in providing Verisign DNSSEC Signing Service for the TLD/GTLD Zone Signing Services. Verisign publishes the DPS in the Repository section of Verisign's website.

B. Components of the System Used to Provide the Services

1. 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 activities related to the lifecycle of the 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 (HSMs) and keying material.

Areas used to create and store cryptographic material enforce dual control, each through the use of two-factor authentication including biometrics. 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.

2. Software

Verisign utilizes commercial and custom developed software to deliver DNSSEC TLD/GTLD Zone Signing Services. Software supporting Verisign's DNSSEC systems' infrastructure includes operating systems (AIX and multiple UNIX/Linux implementations) and databases (Oracle). Internally-developed applications perform product delivery functions. In addition, Verisign uses multiple backup/restore utilities to perform daily and periodic backups of production systems. Backup utilities send e-mail reports indicating whether backups were successfully completed or if the backup failed. Verisign uses the ServiceNow ticketing system to manage its Change Management process. Once submitted, change requests follow a change management workflow, including approval and testing steps, until closed. Verisign uses Nagios to monitor service levels. In addition, Verisign uses tools such as vulnerability scanning and network management software to monitor system availability and performance and to detect suspicious or unusual activities.

3. People

Core Internal Functional Areas
Core functions supporting the DNSSEC systems' infrastructure include:

- Production Operations is responsible for management and operations of systems and networks;
- Physical Security maintains the safety and security of the buildings that house the in-scope systems;
- Critical Facilities is responsible for climate controls, fire suppression, and power-related systems;
- Information Security manages and maintains various security policies, performs risk assessments, and performs monitoring to detect attacks;
- Engineering reviews releases for compliance with standards and manages and controls the Release Management process;
- Enterprise IT is responsible for end-user workstation security, e-mail security, and corporate systems supporting in-scope systems;
- Human Resources performs screening, hiring, and personnel management functions; and
- Technical Project Management defines and controls the project and development life cycle processes.

Trusted Roles
Trusted Persons include employees and non-employees who have access to or control operations that may materially affect:

- Generation and protection of the private component of the TLD/GTLD 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 help 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 help 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.

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 appropriate Trust Anchor.

4. Data

Data as defined for the DNSSEC system includes all electronic data submitted by the customer to Verisign or electronic data generated by Verisign. Verisign internally generates data during the normal operations of the system. The Verisign DNSSEC TLD/GTLD Zone Signing System data consists of the following:

- TLD/GTLD KSK and associated cryptographic activation materials used to protect the KSK;
- TLD/GTLD ZSKs and associated cryptographic activation materials used to protect the ZSK;
- TLD/GTLD Signed Keysets;
- TLD/GTLD Zone File;
- 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's 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).

5. Processes and 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 for the DNSSEC Root Zone 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;
- 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;
- Personnel management, including maintaining the personnel component of business continuity, assessing the integrity and skills of employees, and disciplining employees;
- Key management operations, including key generation, key storage, key archival, key destruction and key usage.

Key Management

The Verisign DNSSEC TLD/GTLD ZSK and KSK key pair generation is performed by trusted individuals using pre-planned key generation ceremonies. HSMs used for ZSK and KSK key pair generation are validated at FIPS 140-2 level 3. 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 private keys are stored within hardware cryptographic modules and are not exposed in plain-text outside of the HSM. KSK and ZSK public keys are backed up and archived.

The operational period of TLD/GTLD KSK and ZSK ends when they are superseded, and these keys are 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 TLD/GTLD KSKs are RSA key pairs with a modulus size of 2048 bits, and the current TLD/GTLD ZSKs are RSA key pairs with a modulus size of 1280 bits. The KSK and ZSK signatures are generated by calculating SHA-256 hashes of the data and encrypting that with the private key. Multiple successive ZSKs are signed by the respective KSK once per year. ZSK key rollover is performed quarterly during an automated process, and KSK key rollover is evaluated once a year and is performed when deemed necessary by the DNSSEC Policy Management Authority.

C. Use of Subservice Organizations and Complementary User Entity Controls

1. Subservice Organizations

The Company uses a subservice organization for the following services:

Services Provided
The subservice organization is responsible for hosting services related to the system, including the restriction of physical access to the defined system including, but not limited to, facilities and backup media.

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include the services provided by the subservice organization.

Our conclusion regarding effectiveness of controls within the system to achieve Verisign's service commitments and system requirements based on the applicable trust services criteria assumes that the complementary subservice organization controls assumed in the design of Verisign's Cryptographic Business Office (CBO) and Secure DNS (DNSSEC) System related to the DNSSEC TLD/GTLD Zone Signing System operated effectively throughout the period January 1, 2024 to December 31, 2024.

2. Complementary User Entity Controls

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include complementary user entity controls.

Our conclusion regarding the effectiveness of controls within the system to achieve Verisign's service commitments and system requirements based on the applicable trust services criteria assumes that complementary user entity controls assumed in the design of Verisign's controls operated effectively throughout the period January 1, 2024 to December 31, 2024.

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 DNSSEC TLD/GTLD Zone Signing 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 the TLD/GTLD Zone. The DPS states the practices and provisions that Verisign employs in providing Verisign DNSSEC Signing Services for the TLD/GTLD Zone Signing Services.

Verisign's service commitments and system requirements related to security, availability, and processing integrity include, but are not limited to, the following:

- Protection of user entities' information against unauthorized access, modification, or disclosure;
- Providing for the availability of system supporting user accounts and user entity data; and
- Processing Integrity principles which are designed to support complete, valid, accurate, timely, and authorized system processing.

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 within 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 on how to carry out specific manual and automated processes required in the operation and development of the DNSSEC Services have been documented.