Internet Corporation for Assigned Names and Numbers (ICANN)

Root Zone Key Signing Key Operator System

System and Organization Controls Report

Report on ICANN's Assertion on the Root Zone Key Signing Key Operator System and on the Suitability of the Design and Operating Effectiveness of Controls to Meet the Criteria for Security, Availability and Processing Integrity

Throughout the Period December 1, 2022, to November 30, 2023

RSM US LLP

I. Independent Service Auditor's Report

To management of Internet Corporation for Assigned Names and Numbers:

Scope
We have examined Internet Corporation for Assigned Names and Numbers' (ICANN's) accompanying assertion in Section III, titled "Assertion of Internet Corporation for Assigned Names and Numbers' Management," (assertion) that the controls within ICANN's Root Zone Key Signing Key Operator system (system) were effective throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that ICANN'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*, in AICPA *Trust Services Criteria*.

ICANN uses a subservice organization identified in the assertion to provide data center housing services. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ICANN, to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria. The assertion presents the types of complementary subservice controls assumed in the design of ICANN's controls. The assertion does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities
ICANN 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 ICANN's service commitments and system requirements were achieved. ICANN has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ICANN is responsible for selecting, and identifying in its assertion, the applicable trust services 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 AICPA. 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.

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

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 ICANN'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 ICANN'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 ICANN's Root Zone Key Signing Key Operator system were effective throughout the period December 1, 2022, to November 30, 2023 to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RSM US LLP

Los Angeles, California
July 16, 2024

II. Assertion of Internet Corporation for Assigned Names and Numbers' Management

We are responsible for designing, implementing, operating and maintaining effective controls within Internet Corporation for Assigned Names and Numbers' (ICANN's) Root Zone Key Signing Key Operator System (system) throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that ICANN'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, in AICPA Trust Services Criteria. 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 December 1, 2022, to November 30, 2023, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria. ICANN'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.

ICANN uses a subservice organization identified in the attached description of ICANN's Root Zone Key Signing Key Operator System provide data center housing services. The attached description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ICANN, to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria.

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 December 1, 2022, to November 30, 2023, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Internet Corporation for Assigned Names and Numbers' Description of the Root Zone Key Signing Key Operator System

Company Background

Internet Corporation for Assigned Names and Numbers (ICANN) has approximately 460 staff based in four regional offices, four engagement centers and its headquarters in Los Angeles. ICANN's leadership is composed of 11 executives reporting to ICANN's interim president and chief executive officer (CEO).

To enhance the security of the domain name system (DNS), ICANN, through its affiliate Public Technical Identifiers (PTI), operates the Root Domain Name System Security Extensions (DNSSEC) key management process. DNSSEC strengthens authentication in DNS using digital signatures based on public key cryptography.

ICANN contracts with the Internet Engineering Task Force (IETF) and the five Regional Internet Registries (RIRs) to provide the Internet Assigned Numbers Authority (IANA) functions. Through the contractual terms between PTI and ICANN, PTI is responsible for performing the IANA functions, performing third-party audits of the Root Zone DNSSEC Key Signing Ceremonies and maintaining the Registry Assignment and Maintenance Systems.

System Overview

Root Zone Key Signing Key Operator System Description

To enhance the security of the DNS, ICANN, through its affiliate PTI, operates the Root DNSSEC key management process. The Root Zone Key Signing Key Operator System (RZ KSK System) is used to manage the Root DNSSEC key, which includes the generation, storage, usage, destruction and backup of the key signing key (KSK) for the DNS root zone. The RZ KSK System's operations are performed inside secure facilities using Federal Information Processing Standards (FIPS) 140-2 Level 4 cryptographic hardware security modules (or HSMs).

Overview of Services Provided

Key Management Operations Overview

RZ KSK System operations are performed in formal key ceremonies. These key ceremonies typically occur four times per year. Between key ceremonies, components are stored in secure safes within the secure facilities in a powered-off state. The KSK is generated during key ceremonies and is also used to sign zone signing keys (ZSKs) from the Root Zone Maintainer. Ceremony activities are scripted and filmed for observation, and artifacts are accessible to the public. Access to the components is limited by physical access controls and logical access controls. Access and key management operations are formally logged.

Boundaries and Scope of the Report

The scope of this report includes the security, availability and processing integrity categories and the related controls for ICANN's RZ KSK System that support the achievement of the service commitments and system requirements based on the applicable trust services criteria. The boundaries of the system begin with the commencement of the quarterly key signing ceremony led by the designated ceremony administrator (CA).

Data enters the boundaries of the system when the dedicated ceremony computer is powered on and the operating system media and HSM are connected via USB. The boundaries of the system end at closing of the key signing ceremony. Data exits the boundaries of the system once the KSK is backed up and returned to secure storage in a tamper-evident bag (TEB).

The ceremony closing procedures include steps to retain the output of the signer system, a copy of the ceremony script, audio-visual recordings of the ceremony, physical access logs and attestations by the designated internal witness (IW) and system administrator (SA).

ICANN uses subservice organizations to host two fully functional, geographically and logically dispersed sites known as key management facilities (KMFs). At any point in time, the KMFs, where the key signing ceremonies are held, hold the data required for production and are evenly utilized. The description does not include any of the controls implemented at the subservice organization.

All sites implement the same physical security protections and operational controls as specified in the DNSSEC Practice Statement. The physical access control systems and security staff reviews are implemented for each KMF but are not included in the description.

Infrastructure and Software

The components used to execute the ceremony include the HSM, smartcards, a specially configured computer and operating system media. None of the aforementioned components are connected to the internet, and are solely used to carry out the KSK ceremonies. There are no users with logical access to these components, the components are not modifiable and are stored in designated safes at the KSK ceremony sites.

The following table describes the components within the scope of the report, utilized in support of the key signing ceremonies:

Component	Process/Transactions	Purchased or Developed
Hardware security model (HSM)	The HSM is a device used for key management and cryptographic functions. The HSM is certified with the highest level FIPS 140 security certification at Security Level 4 Overall. The HSM is stored in the designated equipment safe in tamper-evident packaging. A minimum of three out of seven HSM smartcards are required to enable the HSM and to perform functions involving the KSK. The primary purpose of the HSM is to store the DNSSEC root key. Each HSM is stored in a TEB that is held in a designated safe at each site where the KSK ceremonies are conducted.	Purchased
Computer	A specially configured computer is used to support key signing functions during the ceremony. During each ceremony, the computer is validated to ensure that it has no hard drive and no battery. The computer is configured for the sole use of carrying out the KSK. The computer is stored in a TEB and stored in the designated equipment safes at the sites where the KSK ceremonies are conducted.	Purchased
Operating system media	The operating system media is used to support the key signing functions during the ceremony through the specially configured computer above. The operating system media is validated during each ceremony. An image of the media is available on ICANN's website where the public may access it and recalculate the cryptographic hash to verify it is a true and correct copy.	Developed

Component	Process/Transactions	Purchased or Developed
	The operating system media is kept in a TEB and is stored in the designated equipment safes at the sites where the KSK ceremonies are conducted.	
Smartcards	The smartcards are used during the ceremony in conjunction with the HSM to support cryptographic functions. A combination of authorized smartcards handled by trusted community representatives is required to activate the HSM. The smartcards are stored in TEBs and are stored in the designated equipment safes at the sites where the KSK ceremonies are conducted.	Purchased

Authorized individuals with physical keycard access and the safe combinations can access the aforementioned components. Access to the tiers within the KMFs is monitored through badge access systems and video surveillance, and the physical access systems are configured to trigger alarms if motion is detected outside of the designated KSK ceremony time. Notifications are sent to management if alarms are triggered.

Security Controls

ICANN ensures that the systems maintaining key software and data files are secure from unauthorized access through storage in TEBs in secured safes when not in use. Access is restricted to those individuals with physical access to the the data centers hosted by the subservice organizations, which are also where the key signing ceremonies are held.

Network Security Controls

No part of the signer system making use of the HSM is connected to any communications network.

Communication of ZSK signing requests from the Root Zone Maintainer is done using a client-side authenticated web server connected to ICANN's production network. Transfer of a key signing request from the web server to the signer system is performed manually using removable media. ICANN's production network is logically separated from other components. This separation prevents network access except through defined application processes. ICANN 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. Firewall configurations for the infrastructure components used during the key signing ceremony are reviewed following each ceremony.

People

ICANN has approximately 460 staff based in four regional offices, four engagement centers and its headquarters in Los Angeles. Its executive leadership is composed of senior executives reporting to ICANN's interim president and CEO. Each executive has a management team responsible for the departments and teams reporting to them. An organization chart is maintained by global human resources and is made available to staff on the company intranet. The staff responsible for the performance of the IANA services are employed by PTI, an affiliate of ICANN.

Ceremony Roles Defined as Trusted Persons

Trusted persons, an integral element of key ceremonies, are composed of respected community members and authorized ICANN and PTI staff. Access to, and use of the KSK throughout the ceremony is subject to multiparty control amongst these trusted persons. Trusted persons include all staff, contractors and consultants that have access to or control operations that may materially affect the generation and protection of the private component of the KSK, secure export or import of any public components, and zone file data integrity.

Trusted roles include but are not limited to:

Ceremony Administrator (CA): A CA leads each key signing ceremony and is responsible for conducting a ceremony in accordance with the script. The CA performs many of the steps of the script directly or guides the other participants to fulfil their responsibilities, including escorting participants between facility tiers. It is the CA's responsibility to decide on proper actions after consulting with the internal witness regarding any exceptions to the ceremony script.

Internal Witness (IW): An IW is responsible for attesting that a ceremony has been executed as described in the ceremony script. The IW supports the CA in escorting ceremony participants and fulfilling dual occupancy requirements for the facility tiers.

Crypto Officer (CO): A CO is a trusted community representative that is individually responsible for overseeing one of seven key shares per facility required to activate the secure materials in the HSM device, plus provides general oversight of the KSK management to improve confidence and acceptance in the DNSSEC security mechanism among the wider internet community. The CO is not affiliated with PTI, ICANN or Verisign.

Recovery Key Share Holder (RKSH): An RKSH is individually responsible for securely maintaining one of seven key shares of the storage master key (SMK) used for disaster recovery purposes. The shares are geographically dispersed and are stored in a smartcard in tamper-evident packaging. Each RKSH is entrusted to ensure physical security of the key share.

Safe Security Controller (SSC): An SSC controls access to a safe in the ceremony room. The safes contain the HSM devices, access credentials and other equipment.

System Administrator (SA): An SA operates support systems used in the ceremony, including the access control system and audio-visual equipment. The SA has the competence to resolve technical failures should they arise and may also escort visitors within the KMF.

Second Ceremony Administrator (CA Backup) and Second Internal Witness (IW Backup): These participants satisfy dual-occupancy rules in the ceremony room when the CA and IW are in the safe room. They may step in as CA or IW in the event that the primary CA and IW are unable to fulfill their roles, and may otherwise aid in logistics.

Roles Defined as not Trusted Persons

The following roles are deemed not trusted, meaning the individuals fulfilling these roles do not have access to or control operations that may materially affect generation or protection of the private component of the KSK, secure export or import of any public components, and zone file data integrity. Non-trusted roles include but are not limited to:

ZSK representative: This is the representative of the Root Zone Maintainer, which maintains the Root ZSKs.

External witness (EW): The EW is not affiliated with ICANN and is present at a ceremony to observe and attest that the ceremony has been executed as described by the ceremony script.

Staff witness (SW): The SW is affiliated with PTI or ICANN and observes a ceremony and attests to whether the ceremony has been performed as described in the ceremony script.

Third-party auditor (AUD): Like the EW, the auditor is not affiliated with ICANN and observes the ceremony to attest that it has been executed as described by the ceremony script. This role is associated with the party performing the System and Organization Controls (SOC) 3 attestation.

Policies and Procedures

ICANN has established, maintained and enforced control procedures to ensure that segregation of duties is based on roles that require multiple trusted persons to perform sensitive tasks, such as access to and management of cryptographic key material. In an effort to provide an overall direction regarding execution of each ceremony, ICANN has developed, documented and implemented a wide array of policies that cover the security, availability and processing integrity of its RZ KSK System. These include, but are not limited to:

- Key Management Policy
- Key Management Procedures
- KSK Emergency Rollover Plan

The principal steps during a ceremony include the following:

- Ceremony participants enter the secure KMF.
- Authorized individuals remove cryptographic components from secure safes.
- Cryptographic components are assembled by authorized staff inside the ceremony room.
- The KSK is generated, used to sign the ZSK, destroyed or a combination of these actions.
- Components are powered off, disassembled and returned to secure safes.
- Key ceremony participants leave the secure KMF

Key Management Facilities

The RZ KSK System resides within physically protected environments that deter, prevent and detect any unauthorized use of, access to or disclosure of sensitive information and systems, whether covert or overt. ICANN maintains disaster recovery capabilities for its DNSSEC operations by maintaining two sites with comparable physical security. Both facilities, which are hosted by the subservice organizations, are separated geographically and utilized in alternating ceremonies to ensure that supporting systems are operational.

The RZ KSK System is protected by multiple tiers of physical security, with access to lower tiers required before gaining access to higher and more-restrictive tiers. Key management operations occur within the following physical tiers:

Tiers 1–2

These tiers control external access into the secure KMF. These tiers are managed by the third-party co-location subservice organization. Physical access is logged, and only authorized staff are allowed to enter the facilities unescorted. Unescorted staff, including visitors or staff without authorization, are not allowed beyond these security tiers. The scope of this report does not include the processes performed by the co-location subservice organization, as it is responsible for the control of access to its facilities.

Tiers 3–5

These tiers control access within the KMF, and are controlled by ICANN. Physical access is logged and video is recorded. These tiers enforce individual access control through the use of two-factor authentication. Unescorted staff, including visitors or staff without authorization, are not allowed into these secured areas. Access to these security tiers is restricted in accordance with ICANN's segregation of duties requirements, which require several individuals to access the components within these tiers.

Tiers 6–7

These security tiers control access to the HSMs and operator cards. These cryptographic components are protected through the use of locked safes, TEBs and safe deposit boxes. Access to these security tiers is restricted in accordance with ICANN's segregation of duties requirements, which require several individuals when accessing the components within these tiers. These security tiers also include physical safe deposit boxes that secure HSM credential cards. Access to these safe deposit boxes requires physical keys, which are distributed to and safeguarded by COs.

Data

ICANN maintains a documented KSK information security policy that is reviewed by management annually and available on the IANA public-facing website. The information security policy contains policies and procedures over information classification and handling.

Information that has been entrusted in relation to the RZ KSK operator function is to be protected in a manner commensurate with its sensitivity and critically. Security measures are employed based on the media on which information is stored, the system that processes the information, or methods by which the information is moved. The following records shall be kept confidential and private:

- Private keys and information needed to recover such private keys
- Signatures of key sets to be published in the future
- Transactional records (both full records and the audit trail of transactions)
- Audit trail records created or retained by the RZ KSK operator or the RZ ZSK operator
- Audit reports created by the RZ KSK operator or the RZ ZSK operator (to the extent such reports are maintained), or their respective auditors (whether internal or public), until such reports are made public
- Security measures controlling the operations of the RZ KSK operator's hardware and software and the administration of DNS Keys

Subservice Organizations

ICANN uses a subservice organization for co-location data center housing services and managed services. The scope of this report does not include the controls and related trust service criteria at the subservice organization. The following table presents a description of services the subservice organization provided:

Subservice Organization	Service Provided
Equinix	Data center housing services for the East KMF and West KMF, where the KSK ceremonies are held in Culpeper, Virginia, and Los Angeles, California, respectively

Below are the applicable trust service criteria that are impacted by the subservice organization and the controls expected to be implemented at the subservice organization.

Applicable Criteria	Controls Expected to Be Implemented
Common Criterion 6.4 The entity restricts physical access to facilities and protected information assets	• Access to the facility is restricted to staff or visitors authorized by the tenant and reviewed periodically by management for appropriateness.

Applicable Criteria	Controls Expected to Be Implemented
(for example, data center facilities, backup media storage, and other sensitive locations) to authorized staff to meet the entity's objectives.	• The ability to administer the badge access control system is restricted to user accounts accessible by authorized staff. • Visitors are required to be escorted by authorized staff while within the co-location facilities. • Badge access privileges are provisioned or revoked according to ICANN requests.
Common Criterion 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	• Events are reported to clients as needed to assist with resolving security and availability incidents.
Common Criterion 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents, as appropriate.	• Events are reported to clients as needed to assist with resolving security and availability incidents.
Availability Criterion 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	• Critical components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. • Hot sites, warm sites and cold sites are maintained for system failover. • Environmental monitoring software is configured to monitor cooling systems, uninterrupted power supply (UPS), smoke detectors, sprinklers and fire suppression systems.
Availability Criterion 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	• Disaster recovery procedures are documented, reviewed and tested on a periodic basis.

Attachment B

Principal Service Commitments and System Requirements

ICANN designs its processes and procedures related to the Root Zone KSK System based on the service commitments that ICANN makes to user entities and the operational and compliance requirements that ICANN has established.

Security, availability and processing integrity commitments to user entities are documented and communicated in the IANA Naming Function Contract. Security, availability and processing integrity commitments include, but are not limited to, the following:

Security

Security Commitments

- ICANN owns and maintains various security policies covering security, disaster recovery, incident response, and access control.
- ICANN ensures that individuals performing security functions are provided training of appropriate and relevant security and technical topics.
- ICANN adheres to the DNSSEC Practice Statement in managing and providing KSK and key distribution services.
- ICANN generates and protects the private component of the KSK.
- ICANN securely imports public key components from the ZSK operator.
- ICANN securely signs the ZSK keyset.
- ICANN securely transmits the signed ZSK key set to the ZSK operator.

Security Requirements

- Users are subject to ICANN's security policies posted on the ICANN intranet.
- Physical access to tiers is restricted to staff who have been authorized for respective tier access.
- Administrative and staff security measures are implemented to restrict access to tiers, equipment, safe storage, and other components of the system to authorized and appropriate users.
- System security measures are implemented to secure the transmission of data through encryption and network security measures.
- Security measures with third parties and vendors with whom ICANN shares information are implemented to document, control and mitigate risk associated with the use of third parties.

Availability

Availability Commitments

- ICANN provides a stable and secure environment for all functions through the implementation of processes and policies.

- ICANN maintains a disaster recovery plan that is reviewed annually.
- PTI maintains a contingency and continuity operation plan that is reviewed and approved annually.
- ICANN provides redundant sites in at least two geographically dispersed sites within the United States, as well as multiple resilient communication paths to customers to ensure continuation of the IANA naming function in the event of cybersecurity or physical attacks, emergencies or natural disasters.
- ICANN issues an emergency key roll-over within a reasonable time if any private key component associated with the zone is lost or suspected to be compromised.

Availability Requirements

- ICANN ensures the KSK is backed up after creation and alternating KMFs are used for each ceremony to ensure the HSMs at each location are operating effectively.
- ICANN maintains and annually tests the effectiveness of a disaster recovery plan and business continuity plan.
- ICANN maintains two geographically distinct KMFs that are designed, operated, tested and maintained to meet industry-accepted standards for availability and recovery time, as well as meet corporate policies and procedures.

Processing Integrity

Processing Integrity Commitments

- ICANN ensures that procedures and the KSK system description for the KSK are documented, communicated and followed during each ceremony.
- ICANN provides competent staff to manage the KSK.
- ICANN authenticates and validates the public ZSK keyset.

Processing Integrity Requirements

- A detailed process is documented within the ceremony scripts, which is followed during ceremonies.
- After development, the software used to perform KSK operations in a ceremony is subject to an independent third-party code review and posted online for anyone in the public to review.
- Issues reported to ICANN relating to the root zone KSK operations are processed in accordance with the incident handling procedure.