Internet Corporation for Assigned Names and Numbers

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 the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability and Processing Integrity

Throughout the Period
December 1, 2018, to November 30, 2019

RSM US LLP

I. Report of Independent Accountants

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 II, titled "Assertion of ICANN's Management," (the assertion) that the controls within ICANN's Root Zone Key Signing Key Operator System (the system) were effective throughout the period December 1, 2018, to November 30, 2019, 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* (AICPA, *Trust Services Criteria*).

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. In Section II, ICANN has provided the accompanying assertion about the effectiveness of the 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 whether 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are 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 risks 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, 2018, to November 30, 2019, 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

San Francisco, California
April 21, 2020

II. Assertion of ICANN's Management

We are responsible for designing, implementing, operating and maintaining effective controls within ICANN's Root Zone Key Signing Key Operator System (the system) throughout the period December 1, 2018, to November 30, 2019, to provide reasonable assurance that ICANN'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 controls within the system throughout the period December 1, 2018, to November 30, 2019, 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* (AICPA, *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.

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, 2018, to November 30, 2019, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

ICANN's Description of the Root Zone Key Signing Key Operator System Throughout the Period December 1, 2018, to November 30, 2019

System Overview

Root Zone Key Signing Key Operator System Description

To enhance the security of the domain name system (DNS), Internet Corporation for Assigned Names and Numbers (ICANN), through its affiliate Public Technical Identifiers (PTI), operates the Root DNS Security Extensions (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 generation, storage, usage 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 FIPS 140-2 Level 4 cryptographic hardware security modules (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 containers 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 (RZM). Ceremony activities are scripted and filmed for observation and access by the public. Access to the components is limited by physical access controls; there are no logical access controls. Access and key management operations are formally logged.

Boundaries and Scope of the Report

The scope of the 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.

ICANN uses subservices organizations and has implemented at least two fully functional, geographically and logically dispersed sites, which at any point in time hold the data required for production, and are evenly utilized. The description does not include any of the controls expected to be implemented at the subservices organizations.

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 personnel reviews are implemented at Equinix, but are not included in the description.

Computer Security Controls

ICANN ensures that the systems maintaining key software and data files are secure from unauthorized access. In addition, ICANN limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Network Security Controls

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

Communication of ZSK key signing requests from the RZM/ZSK operator 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.

Infrastructure

The RZ KSK operating system (OS) relies on specific hardware that, in between key ceremonies, is individually kept in tamper-evident bags and stored in secure containers within the secured facilities in a powered-off state. The hardware critical to performing a Root Zone key ceremony includes:

- **HSM Device:** The HSM device is used for key management and performing encryption functions. The HSM is certified with the highest level of 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 private key.

- **Smartcards:** The smartcards are used during the ceremony in conjunction with the HSM in order to support encryption functions. A combination of authorized smartcards handled by the trusted community representatives is required to activate the HSM. The smartcards are stored in tamper-evident bags and are stored in the designated credentials safe.

- **Laptop:** A specially configured laptop is used to support key signing functions during the ceremony. The laptop is stored in tamper-evident packaging and stored in the designated equipment safe. During each ceremony, the laptop is validated to ensure that it has no hard drive and no battery. The laptop relies on an OS DVD that is also validated during each ceremony.

- **OS DVD:** The OS DVD used by the laptop is kept in tamper-evident packaging and is stored in the designated equipment safe. The OS DVD is validated during each ceremony. An image of the DVD 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.

Software

The OS DVD contains the software necessary for the laptop to support encryption functions. Should any changes be made to the OS DVD software, it is subject to an independent third-party code review and posted online for anyone in the public domain to review.

People

ICANN has approximately 400 personnel based in four regional offices, four engagement centers and its headquarters in Los Angeles. Its leadership is composed of 13 executives reporting to ICANN's president and chief executive officer. Each executive has a senior management team to manage the departments reporting to them. An organization chart is maintained by the human resources (HR) department and is made available to employees on the company intranet. The personnel 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 the key ceremony, are comprised of respected community members and authorized ICANN and PTI personnel. Access to, and use of the KSK throughout the ceremony is subject to multiparty control amongst these trusted persons. Trusted persons include all employees, contractors and consultants that have access to or control operations that may materially affect 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 (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 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):** A RKSH is individually responsible for securely maintaining one of seven key shares of the Storage Master Key (SMK). 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):** A 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 also can escort visitors within the key management facility (KMF).

- **Second Ceremony Administrator (CA2) and Second Internal Witness (IW2):** 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 otherwise may 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:** Representative of the Root Zone Maintainer, which maintains the Root Zone Signing Keys.

- **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:** Similar to the external witness, 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 SOC 3 audit.

Policies and Procedures

ICANN has established, maintained and enforced control procedures to ensure the segregation of duties are based on roles that require multiple trusted persons 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 Rollover Plan

The principal steps during a ceremony include the following:

- Ceremony participants enter the secure key management facility.

- Authorized individuals remove the cryptographic components from secure containers.

- Cryptographic components are assembled by authorized personnel inside the ceremony room.

- The KSK is generated or used to sign the ZSK.

- Components are powered off, disassembled and returned to secure containers.

- Key ceremony participants leave the secure key management facility.

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 are separated geographically and utilized in alternating ceremonies to ensure 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 these physical tiers.

Tiers 1–2

These tiers control external access into the secure key management facility. These tiers are managed by the third-party co-location providers. Physical access is logged and only authorized personnel are allowed to enter the facilities unescorted. Unescorted personnel, including visitors or employees without authorization, are not allowed beyond these security tiers. The scope of this report does not include the processes performed by the co-location provider, Equinix, as it is responsible for the control of access to their facilities.

Tiers 3–5

These tiers control access to the key management facility that is 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 personnel, including visitors or employees without authorization, are not allowed into these secured areas. Access to these security tiers is restricted in accordance with ICANN's segregation of duty 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, tamper-evident bags 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 operator cards. Access to these safe deposit boxes require physical keys, which are distributed to crypto officers.

Attachment B

Principal Service Commitments and System Requirements

ICANN designs its processes and procedures related to the Root Zone Key Signing Key (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 will have proper knowledge and training of required security topics. This also includes security awareness training.
- 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 and privacy policies posted on the ICANN intranet.
- Physical access to tiers is restricted to personnel who have been authorized for respective tier access.
- Administrative and personnel 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 in place, including firewall reviews, data protection systems and system monitoring.
- Third-party security measures include contracts or contract amendments with all partners, third parties and vendors with whom ICANN shares information.

Availability

Availability Commitments

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

- 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 cyber 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 will ensure the KSK is backed up after creation and alternating key management facilities are used for each ceremony to ensure the HSMs at each location are operating effectively.

- ICANN will maintain and annually test the effectiveness of an up to date disaster recovery plan and business continuity plan.

- ICANN will maintain two geographically distinct key management facilities 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.

- 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 within the application or application data are corrected.