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 the security, availability and processing integrity principles throughout the period December 1, 2017, to November 30, 2018

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

Report of Independent Accountants

To the Management of the Internet Corporation for Assigned Names and Numbers:

We have examined management's assertion that Internet Corporation for Assigned Names and Numbers (ICANN), throughout the period December 1, 2017, to November 30, 2018, maintained effective controls over the Root Zone Key Signing Key Operator System (the system) that were suitably designed and operating effectively to provide reasonable assurance that the system:

- was protected against unauthorized access, use or modification
- was available for operation and use as committed and agreed
- was processing completely, validly, accurately, timely and authorized as committed and agreed

based on the criteria for the security, availability and processing integrity principles set forth in TSP Section 100A, *2016 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria) and included as an appendix to this report. ICANN 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 AICPA. 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 ICANN's relevant controls over the security, availability and processing integrity of the 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 of our opinion.

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 at the 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 effectiveness of controls is subject to the risk that controls may become inadequate because of the changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

RSM US LLP

San Francisco, California
March 25, 2019

Internet Corporation for Assigned Names and Numbers’ Assertion

ICANN is responsible for designing, implementing, operating and maintaining effective controls over the Root Zone Key Signing Key Operator System (the system) throughout the period December 1, 2017, to November 30, 2018, based on the criteria to meet the security, availability and processing integrity principles set forth in TSP Section 100A, *2016 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria) as noted in an appendix to this report. ICANN maintained effective controls over the system that were suitably designed and operating effectively to provide reasonable assurance that the system:

- was protected against unauthorized access, use or modification
- was available for operation and use as committed and agreed
- was processing completely, validly, accurately, timely and authorized as committed and agreed

Our attached description of the system identifies the aspects of the system covered by our assertion throughout the period December 1, 2017, to November 30, 2018.

Sincerely,

Internet Corporation for Assigned Names and Numbers

Internet Corporation for Assigned Names and Numbers’ Description of the Root Zone Key Signing Key Operator System Throughout the Period December 1, 2017, to November 30, 2018

System Overview

Root Zone Key Signing Key Operator System Description

To enhance the security of the domain name system (DNS), the Internet Corporation for Assigned Names and Numbers (ICANN), through its affiliate Public Technical Identifiers, 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 generating, storing, using and backing up the Key Signing Key (KSK). The RZ KSK System’s operations are performed inside secure facilities using FIPS 140-2 Level 4 cryptographic hardware security modules (HSMs).

Key Management Operations

RZ KSK System operations are performed in formal key ceremonies. These key ceremonies occur four times per year. In 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 the Zone Signing Key (ZSK)[1] 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. Trusted Persons, an integral element of the key ceremony, comprised respected community members and authorized ICANN personnel. 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 RZ KSK
- Secure export or import of any public components
- Zone file data

Trusted roles include, but are not limited to:

- Designated system administration personnel
- Crypto officers
- Recovery key shareholders
- Safe security controllers
- Internal witnesses
- The ceremony administrators

[1] The ZSK is received from the RZM up to 90 days prior to use. The ZSK is authenticated and validated against the prior signed key set.

Access to, and use of, the KSK throughout the ceremony is subject to multiparty control amongst these Trusted Persons.

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.

The principal steps during a key ceremony include the following:

- Key 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.

Cryptographic Functions

Cryptographic functions involving the KSK, including the KSK generation, backup, storage and usage, are performed within cryptographic hardware security modules (HSMs) that are validated at FIPS 140-2 Level 4. HSM operations occur at formal key management ceremonies. To operate the HSM during these ceremonies, a minimum of three out of seven HSM smart cards are required to enable the HSM and to perform functions involving the KSK private key.

Backups of the KSK are made in the event of an unplanned emergency. The key that is used to encrypt the KSK backups is split into separate components using a “five out of seven” smartcard threshold scheme. The seven smart cards are distributed to geographically dispersed individuals in tamper-evident bags. These individuals are responsible for retaining these cards until notified in the event of an emergency.

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 providers, Equinix and Terremark, as they are 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 duty 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 a separate community of Trusted Persons.

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 TLS 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.

Appendix: Applicable Trust Services Criteria

Principles

- Security—The system is protected against unauthorized access, use or modification to meet the entity's commitments and system requirements.
- Availability—The system is available for operation and use to meet the entity's commitments and system requirements.
- Processing integrity—System processing is complete, valid, accurate, timely and authorized to meet the entity's commitments and system requirements.

Criteria

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.

Ref	Criteria
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 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.

Ref	Criteria
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.
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.

Ref	Criteria
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. This criteria is not applicable to the Root Zone Key Signing Key Operator System since the system and generation of keys is performed offline.
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.

Ref	Criteria
PI1.6	Modification of data, other than routine transaction processing, is authorized and processed to meet the entity’s processing integrity commitments and system requirements. This criteria is not applicable to the Root Zone Key Signing Key Operator System since modifications does not occur outside of the routine (quarterly) key ceremonies.