The Internet Corporation for Assigned Names and Numbers

ICANN

Internet Corporation for Assigned Names and Numbers (ICANN)

Root Zone Key Signing Key Operator System

Service Organization Control 3 (SOC 3) Report

Report on ICANN's Assertion of the Root Zone Key Signing Key Operator System and on the Suitability of the Design and Operating Effectiveness of Controls relevant to the security, availability, and processing integrity principles throughout the period December 1, 2015 to September 30, 2016

Prepared in Accordance with AT 101 pursuant to TSP Section 100A, 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 the Internet Corporation for Assigned Names and Numbers ("ICANN"), throughout the period December 1, 2015 to September 30, 2016, maintained effective controls over the Root Zone Key Signing Key Operator System (RZ KSK System) that were suitably designed and operating effectively to provide reasonable assurance that:

- the RZ KSK System was protected against unauthorized access, use, or modification,
- the RZ KSK System was available for operation and use as committed or agreed, and
- RZ KSK System processing was complete, valid, accurate, timely, and authorized

based on the criteria to meet the security, availability, and processing integrity criteria set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) ("applicable trust services criteria").

ICANN's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ICANN's relevant controls over the security, availability, and processing integrity of the RZ KSK System; (2) testing and evaluating the operating effectiveness of the controls; and (3) examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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

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

PricewaterhouseCoopers LLP

March 2, 2017

The Internet Corporation for Assigned Names and Numbers

ICANN

Management of ICANN's Assertion Regarding Its Root Zone Key Signing Key Operator System throughout the Period December 1, 2015 to September 30, 2016

ICANN operates the Root Zone Key Signing Key Operator System (RZ KSK System), as defined by Management's Description of Its Root Zone Key Signing Key Operator System throughout the period December 1, 2015 to September 30, 2016. In operating the RZ KSK System throughout the period December 1, 2015 through September 30, 2016, based on criteria to meet the security, availability, and processing integrity principles set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Principles and Criteria), ICANN has:

Maintained effective controls that were suitably designed and operating effectively to provide reasonable assurance that:

- the RZ KSK System was protected against unauthorized access, use, or modification,
- the RZ KSK System was available for operation and use as committed or agreed, and
- RZ KSK System processing was complete, valid, accurate, timely, and authorized.

The attached Management's Description of Its Root Zone Key Signing Key Operator System throughout the Period December 1, 2015 to September 30, 2016 identifies those aspects of the system covered by our assertion.

Akram Atallah
President, Global Domains Division

Management's Description of Its Root Zone Key Signing Key Operator System throughout the Period December 1, 2015 to September 30, 2016

Root Zone Key Signing Key Operator System Description

To enhance the security of the domain name system (DNS), ICANN operates the Root Domain Name System Security Extensions (DNSSEC) key management process. ICANN's 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 of the Key Signing Key (KSK). The RZ KSK System's operations occur at 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, are comprised of respected community members and authorized ICANN staff. 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, and
- 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, and
- The ceremony administrators.

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

ICANN has established, and maintains and enforces control procedures to ensure the segregation of duties based on roles and to ensure that multiple Trusted Persons are required to perform sensitive tasks, such as access to and management of cryptographic key material.

The principal steps in a key ceremony include:

- Key ceremony participants enter the Secure Key Management Facility,
- Authorized individuals remove the cryptographic components from secure containers,
- Cryptographic components are assembled in the ceremony room,
- The KSK is generated or used to sign the ZSK,
- Components are powered off, disassembled, and returned to secure containers, and
- Key ceremony participants leave Secure Key Management Facility.

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

Cryptographic Functions

Cryptographic functions involving the KSK, including the KSK generation, backup, storage, and use, 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 smartcards are required to enable the HSM and perform functions involving the KSK private key.

A backup of the KSK is made in the event of an unplanned emergency. The key that is used to encrypt the KSK backup is split into separate components using a "five out of seven" smartcard threshold scheme. The seven smartcards 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.

Secure Key Management Facilities

The RZ KSK System resides within a physically protected environment that deters, prevents, and detects 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 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 3rd 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 key management activity areas 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 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 and 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 to access the components within these tiers. These security tiers include physical safe deposit box keys which are distributed to a separate community of Trusted Persons, and are utilized to access HSM operator cards within the safes.

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 (KSR) from the RZM/ZSK Operator is done using a TLS client-side authenticated web server connected to ICANN's production network. Transfer of a KSR 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 limit the nature and source of network activities that may access production systems that are related to key signing activities.