The Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN)

Root Zone Key Signing Key System SysTrust Report based on the Trust Services Principles of Availability, Security and Processing Integrity

For the Period December 1, 2011 to November 30, 2012

REPORT OF INDEPENDENT ACCOUNTANTS

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

We have examined management's assertion that during the period December 1, 2011 through November 30, 2012, ICANN maintained effective controls over the Root Zone Key Signing Key System (RZ KSK System) to provide reasonable assurance that:

- the system was protected against unauthorized access;
- the system was available for operation and use, as committed or agreed; and
- the system processing was complete, accurate, timely, and authorized

based on the AICPA and CICA Trust Services Security, Availability, and Processing Integrity criteria.

ICANN's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the RZ KSK System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 availability, security and processing integrity of the RZ KSK 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 our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, ICANN's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA Trust Services Security, Availability and Processing Integrity criteria.

PricewaterhouseCoopers LLP
April 25, 2013

The Internet Corporation for Assigned Names and Numbers

Management Assertion on the controls over the Root Zone Key Signing Key (KSK) System based on the AICPA and CICA Trust Services Criteria for Security, Availability & Processing Integrity

ICANN operates the Root Zone KSK System, as defined by the System Description document. In operating the RZ KSK System during the period December 1, 2011 through November 30, 2012, based on the AICPA and CICA Trust Services Criteria for Security, Availability and Processing Integrity, ICANN has:

- Maintained effective controls to provide reasonable assurance that:
  - ✓ the System was protected against unauthorized access
  - ✓ the System was available for operation and use as committed and agreed, and
  - ✓ the System processing was complete, accurate, timely, and authorized

The attached description of the RZ KSK System identifies those aspects of the system covered by our assertion.

Akram Atallah
Chief Operating Officer
April 25, 2013

Management's Description of its Root Zone Key Signing Key System (RZ KSK System) throughout the period of December 1, 2011 through November 30, 2012

Root Zone Key Signing Key System (RZ KSK System) Description

As part of a joint effort between ICANN, VeriSign, and the US Department of Commerce 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 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

All RZ KSK System operations are performed in formal key ceremonies. These key ceremonies occur four times per year. In between key ceremonies, all components are stored in secure containers within the secure facilities in a powered off state. The Key Signing Key (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. All 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. Access to, and use of, the KSK throughout the ceremony is subject to multiparty control amongst these Trusted Persons.

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
- Key ceremony participants leave Secure Key Management Facility

Cryptographic Functions

All cryptographic functions involving the KSK, including the KSK generation, backup, storage, and use, are performed within cryptographic hardware security modules (HSM) that are validated at FIPS 140-2 Level 4. All 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.

[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.

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 facility provider. 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 separate community of Trusted Persons, and are utilized to access HSM operator cards within the safes.