DNSSEC Root Zone
High Level Technical Architecture

Prepared by the Root DNSSEC Design Team

Joe Abley
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
David Knight
Tomofumi Okubo
Jakob Schlyter

Version 1.2.1

October 28, 2009

Requirements

This document describes the proposed architecture for DNSSEC deployment at the root of the DNS resulting from ongoing discussions between VeriSign and ICANN based on requirements set forth by the U.S. Department of Commerce (DoC). It is only meant to be a high-level description of the design. Details are to be contained in accompanying documentation.

The Root Zone system needs an overall security lifecycle, such as that described in ISO 27001, and any security policy for DNSSEC implementation should be validated against existing standards for security controls.

ISO 27002:2005 (formerly ISO 17799:2005) and National Institute of Standards and Technology (NIST) SP 800-53 are recognized sources for specific controls are considered in the development of the system. Note that reference to SP 800-53 is used as a convenient means of specifying a set of technical security requirements.[1] It is expected that the signing systems referenced in this document will meet all the SP 800-53 technical security controls required by a HIGH IMPACT system.[2]

These Special Publications (SP) and Federal Information Processing Standards (FIPS) documents are not intended as a future auditing checklist, but as non-binding guidelines and recommendations to establish a viable IT security policy. All of the NIST document references can be found on the NIST Computer Security Research Center web page (http://www.csrc.nist.gov/).

Roles and responsibilities

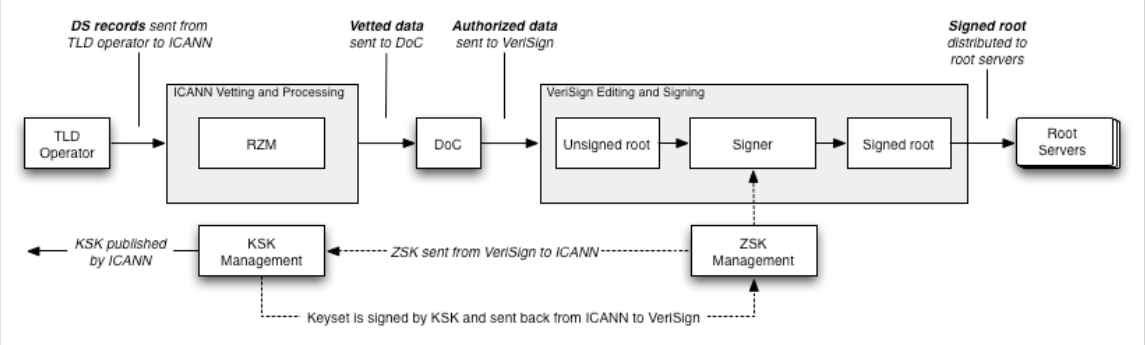

Figure 1

Referring to Figure 1.

ICANN, as part of its performance of the IANA functions, is the interface to Top Level Domain (TLD) operators and is responsible for vetting and processing TLD

[1] Note in particular that the use of the requirements in SP 800-53 does not imply that these systems are subject to other Federal Information Security Management Act (FISMA) processes.

[2] For the purpose of identifying SP 800-53 security requirements, the Root Zone system can be considered a HIGH IMPACT system with regards to integrity and availability as defined in FIPS 199.

DNSSEC public key data. ICANN is also responsible for management of the root zone Key Signing Key (KSK), including generation, publication, and use for signing in cooperation with the Internet community.

The DoC National Telecommunications and Information Administration (NTIA), as part of its role, is responsible for authorizing changes to the root zone file. In the case of DNSSEC, NTIA authorizes the incorporation of TLD DNSSEC public key material (DS records[3]) and KSK-signed key material (the root key set[4]) into the root zone file.

VeriSign, per its Cooperative Agreement with DoC in its role as root zone maintainer, is responsible for incorporating the NTIA-authorized DNSSEC-related changes into the root zone file, signing the file with the Zone Signing Key (ZSK), and distributing the resulting signed root zone file to the root servers. VeriSign is solely responsible for the ZSK.

DS Record Flow

Referring to Figure 1.

As per DoC requirements, DNSSEC public key material provided by the TLD operator is vetted and processed by ICANN and incorporated into a DS change request. When the system is deployed initially, the DS change request will take the form of an email template. ICANN will send the DS change request template to DoC for authorization and to VeriSign for implementation using PGP-signed email. ICANN and VeriSign are working to automate the root zone change management process, and after the deployment of the new root zone automation system, ICANN will communicate DS change requests (and all other root zone change requests) to VeriSign using EPP (the Extensible Provisioning Protocol).

After DoC authorization, VeriSign adds the DS records in the change request to the unsigned root zone file. VeriSign's DNSSEC signing process adds the root key set (which is signed by the KSK) and signs the rest of the root zone with the ZSK. The signed zone is distributed to the same root servers, using the same process, as the unsigned root zone file is currently published.

KSK/ZSK Key Flow

Referring to Figure 1.

VeriSign generates the ZSK and uses it to sign the root zone. ICANN, with participation from the Internet community, generates the KSK and uses it to sign root key sets.

To obtain signed root key sets, VeriSign generates a Key Signing Request (KSR) for ICANN that requests a series of signed key sets with overlapping validity periods. The KSR is described by an XML document and contains the public half of the ZSKs to

[3] The Delegation Signer (DS) record is a cryptographic short-hand representation, or hash, of the TLD's KSK.

[4] The term *key set* refers to a zone's apex DNSKEY RRSet, i.e., the zone's published KSK(s) and ZSK(s).

be signed, signatures made with the private half of the ZSKs to demonstrate private key ownership, the period over which the requested signatures are valid, and other key policy information.

As part of ensuring the integrity and authenticity of the exchange an overall hash of the KSR is calculated for subsequent human verification.. KSR exchanges between VeriSign and ICANN use a client-side SSL authentication mechanism to further preserve the authenticity and integrity of the exchange. (See details below.)

Because DNSSEC signatures have a specific temporal validity period and eventually expire, KSR exchanges will be performed well in advance of the need for KSK signatures to ensure sufficient time for the processing described above.

KSK Publication

In order to ensure broad and accurate dissemination of the public half of the root KSK, ICANN will deploy a web site as at least one means of publication. The KSK will be published on the web site at least 30 days before the start of the next KSK rollover cycle and as soon as possible after the key ceremony generating the new KSK. To simplify incorporation into automated systems, the Web site will include a representation of the KSK as part of an XML document, as well as in standard DNSKEY and DS format.

To demonstrate ownership of the private half of the KSK, a self-signed certificate signing request (PKCS#10 CSR) based on the KSK will also be available on the site. This CSR is also be the primary output of the KSK generation ceremony.

The XML document will be signed by ICANN using PGP and S/MIME (PKCS#7). These signatures will be detached and published at the ICANN website.

The CSR will be processed by the ICANN Certificate Authority and the result, a X.509 certificate, will be published at the ICANN website.

Other certificates and detached signatures by third parties interested in supplying their own attestations may also be included on the site for reference.

The site will also provide a history of KSKs and signatures to facilitate isolated DNSSEC implementations to “catch up”.

DNSSEC Protocol Parameters

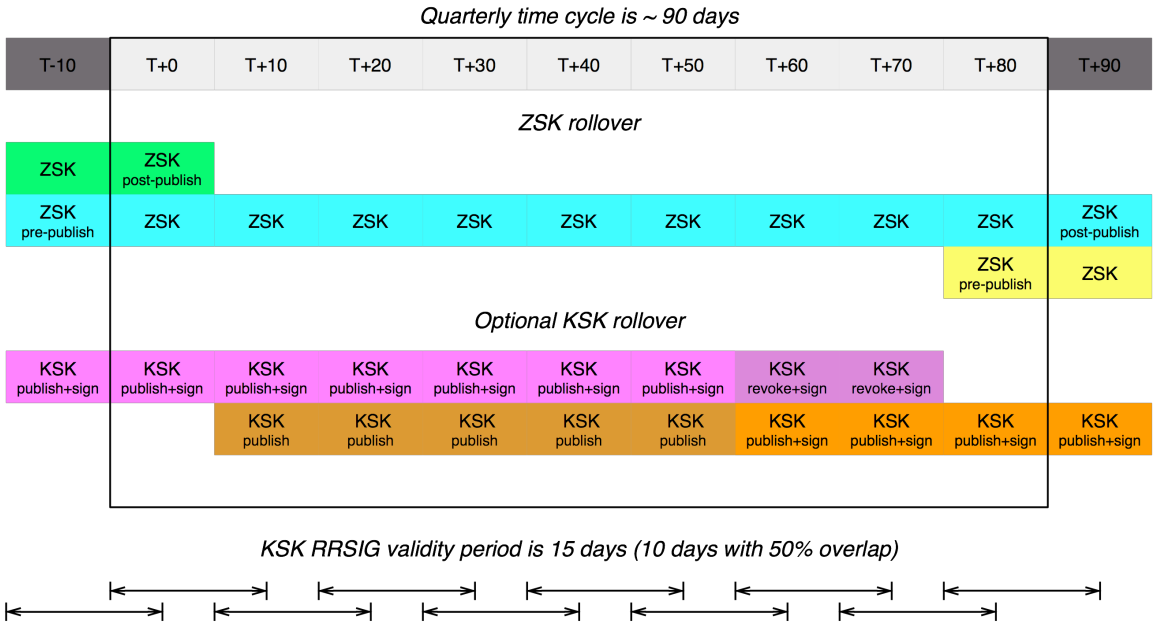

Figure 2

DNSSEC Parameters

The DNSSEC root zone system will use 2048-bit RSA KSKs and 1024-bit RSA ZSKs. The signature algorithm will be RSA-encrypted SHA-256 hashes. Given NIST and other guidelines[5] pressing for use of SHA-256 by end of 2010, and the time frame expected for signing the root zone along with the existence of multiple validator implementations waiting only for algorithm code point assignment, selection of RSA/SHA-256 is deemed by the design team as a stable alterative to forced algorithm rollover in the near term.

The root zone will use NSEC (as opposed to NSEC3) records to provide authenticated denial of existence.

Key Rollover

Referring to Figure 2.

ZSKs (green, blue, yellow in Figure 2) are rolled over quarterly, with each ZSK cycle lasting approximately, but never less than, 90 days. ZSKs are published ten (10) days before use and remain published ten (10) days after use to account for cached entries in the DNS and facilitate rollover. VeriSign submits a KSR containing the ZSK for the next quarterly period (i.e., starting at T+0 in Figure 2) between 30 and 90 days prior to the start of the next period (i.e., between T-90 and T-30). This submission date allows

[5] http://csrc.nist.gov/publications/drafts/800-57-part3/Draft_SP800-57-Part3_Recommendationforkeymanagement.pdf

sufficient time for ICANN to conduct a KSR signing ceremony and return the KSK-signed result to VeriSign to prepare for the signed key sets' inclusion in the signed root.

KSKs (purple, orange in Figure 2) are rolled approximately every two to five years when appropriate, e.g., when current signature algorithms and/or parameters are considered weak (e.g., ECC/SHA3 algorithm deployment, new key lengths, etc.), the current key is believed to be compromised, hardware security module (HSM) upgrade or replacement, or to exercise rollover mechanisms. New KSKs are propagated into the root as part of the regular KSR exchanges but have the additional requirement of NTIA authorization. This authorization step will be facilitated through a secured, specialized web site.

A new KSK is published in the zone 50 days prior to use (i.e., T+10) and remains published 20 days after it is no longer used to sign., i.e., until T+70. (Note that the KSK is published out-of-band on the web site a minimum of 30 days prior to appearing in the zone as described above.[6]) This process facilitates both manual and RFC 5011 automated rollover mechanisms.

The timing of KSK rollovers is chosen to center around normal quarterly ZSK rollover cycles to limit the size of the DNSKEY RRSet to no more than three (3) keys at any one time (i.e., old KSK, new KSK and current ZSK). Furthermore, only the KSK signatures over the DNSKEY RRSet will be generated.[7] These measures keep root zone response packet sizes as small as possible.

KSR Exchange

Referring to Figure 1.

To ensure the integrity and authenticity of the exchange an overall hash of the KSR is calculated for subsequent human verification before transmission to ICANN. ICANN responds with a Signed Key Response, or SKR, containing the KSK signed DNSKEY RRSet. KSR exchanges between VeriSign and ICANN use a client-side SSL authentication mechanism to further preserve the authenticity and integrity of the exchange.

On reception, ICANN verifies the ZSK signatures within the KSR, compares ZSKs within the KSR with ZSKs in the last SKR to validate their origin, and checks the KSR contents against published polices regarding parameters and signature validity periods. ICANN then performs a final manual check involving out-of-band communication of the hash with VeriSign[8] before signing the ZSKs in the KSR with the KSK. For each requested signature in the KSR, ICANN extracts the ZSK(s) and adds the appropriate KSK(s) to form a complete root DNSKEY RRSet. ICANN then signs the key set with the KSK and adds it to the resultant SKR. This process is conducted as part of a signing ceremony at a secure facility involving witnesses and trusted individuals

[6] In the case of an emergency KSK rollover, validator operators will have only the 30 day out-of-band KSK publication period before the new KSK is used to start signing key sets.
[7] Some DNSSEC signers also sign a zone's DNSKEY RRSet with the ZSK.
[8] For example, ICANN and VeriSign could each calculate a cryptographic hash of the KSR and two people (one from each organization) who recognize each other's voices could compare the hash over the phone.

from the Internet community. (More information about the signing ceremony follows in a later section.)

On reception, VeriSign validates the DNSKEY RRSet against the public KSK and verifies parameters and signature validity periods, If a new KSK is being introduced in this KSR, VeriSign places the SKR on an SSL-protected Web site[9] and automatically notifies NTIA via email of SKR awaiting authorization. VeriSign then extracts signed key sets from the SKR for eventual inclusion in the root zone file and subsequent signing and publication of the signed root zone.

Validity Periods

Referring to Figure 2.

In order to recover quickly from possible ZSK compromise and support flexible key rollover schedules, the KSK signatures over the root key sets have a fifteen (15) day validity period, including up to five days of overlap over successive key sets for continuity.

The validity period of signatures made with the ZSK will be between seven and ten (7-10) days to provide sufficient time to recover from equipment and communication failure while limiting the window for replay attacks.

Root Zone Timing Parameters

Root Zone TTL and timing parameters are as follows:

Zone Published	Every 12 hours
Root NS TTL	6 days
Root DNSKEY TTL	**48 hours**
TLD NS TTL	48 hours
TLD DS TTL	**24 hours**
Glue (A and AAAA) TTL	48 hours
SOA TTL	24 hours
NSEC TTL	**24 hours**
Negative caching interval	24 hours

Bold text represents parameters new to the signed root zone.

[9] The web site uses a user name and password and also client-side SSL authentication to control access to the page and cryptographically attest to NTIA's authorization.

Key Administration

All keys will be generated and stored inside hardware security modules (HSMs) validated to FIPS 140-2 level 4 as per DoC requirements. All cryptographic operations making use of private keys (e.g. signing) will be performed inside the HSM. The private portion of the keys never leaves the HSMs in unencrypted form. Any tamper attempt results in the automatic destruction of all key material inside the HSM.

Key Activation

Activation data needed to make use of the private keys inside the HSMs is split into smart cards controlled by multiple trusted individuals. For ZSK operations, these individuals will be employed by VeriSign. For KSK operations, these individuals will be chosen from a pool of trusted members of the Internet community not already part of the root zone management process (i.e., ICANN, VeriSign and the U.S. government). The pool is drawn from members of entities such as:

- ICANN ccNSO (Country Code Names Supporting Organization)
- ICANN GNSO (Generic Names Supporting Organization)
- IAB (Internet Architecture Board)
- RIRs (Regional Internet Registries)
- ISOC (The Internet Society)
  (These entities are given as examples. The exact list has yet to be determined.)

A threshold number of smart cards (m) out of the total number of smart cards (n) created and distributed for a particular HSM is required to activate a private key stored on the module. The threshold number of cards needed to generate or sign with a ZSK or KSK is three (3) out of seven (7). These cards are created and distributed at HSM initialization time and require the parties to sign an agreement acknowledging their crypto officer responsibilities.

Key Backup

For purposes of disaster recovery in which all HSMs at all sites fail, material needed to reconstitute an uninitialized HSM is backed up. All private key backups are encrypted with an internal HSM key, which is backed up separately at HSM initialization time.

For the ZSK, these are in the form of smart cards kept at a secure off-site facility.

For the KSK, the internal HSM key used to encrypt private keys for off-site backup is backed up using a five (5) of seven (7) threshold scheme with the smart cards distributed to organizationally separate parties drawn from the same pool above but not including ICANN, VeriSign nor the U.S. government. The parties keep the cards (in tamper-evident packaging) in geographically dispersed locations under their control. The parties will again sign agreements acknowledging their crypto officer responsibilities. The encrypted backup of the private keys is kept at a secure off-site data storage facility

(in tamper-evident packaging) contracted by ICANN and updated when new keys are generated.

Key Ceremonies

All KSK key management operations will be conducted in the form of key ceremonies conducted inside the secure facilities where the HSMs are kept. The operations include HSM initialization, new key generation, KSR signing, and private key (HSM) destruction. In addition to the required number of crypto officers described above and security officers responsible for physical security, there will be a Ceremony Administrator to manage the process (e.g. run through a checklist) and Internal Witness to formally attest (via Notary) that the published procedures have been properly followed. External witnesses may also be present. Every step is logged and filmed for public viewing and transparency as well as auditing purposes. Logs (automatic and manual) will be audited annually by at least one established external auditor. The ceremonies will alternate between mirror sites to exercise their operational readiness in case of emergency.

Key generation and signing ceremonies will occur well in advance of the intended use of the result (new KSK or signed KSR) and will require a minimum of three (3) of the seven (7) crypto officers controlling the HSM activation smart cards to be present. Due to the frequent (at least twice daily) nature of root signing with the ZSK, this will be a regularly scheduled activity.

Once a new KSK is generated during a key generation ceremony, it is backed up in encrypted form on a smart card and distributed to the mirror site for import. Finally, the smart card backup is placed in tamper evident packaging and stored at the off-site data storage facility. The key ceremony is inclusive of these events and is not deemed complete until they have all been performed.

Key signing ceremonies (during which the contents of the KSR are signed) are more frequent than key generation and, though they alternate between sites, a given signing ceremony does not involve the corresponding mirror site. Because the facility and equipment are offline, the signed KSR and the resulting signed KSR response are transported to and from the facility via removable media by ICANN IT staff.

HSM initialization may occur in conjunction with a key generation ceremony and will require the full complement of all crypto officers (those involved in generation, backup, signing, and destruction) to be present, as well as new crypto officers slated to replace current ones. Creation of HSM activation smart cards, internal HSM encryption key backup, backup of HSM configuration, (re)distribution of keys, and crypto officer agreement signing all happen at these events.

During the destruction of an HSM, which may occur in conjunction with a key generation ceremony, all crypto officers will be present in addition to the Ceremony Administrator and Internal Witness to attest to the destruction of the private keys. HSM destruction is accomplished by both erasure of all keys with the assistance of the crypto officer smart cards and tampering the HSM. The unit will then be returned to the vendor for recycling.

Physical Security

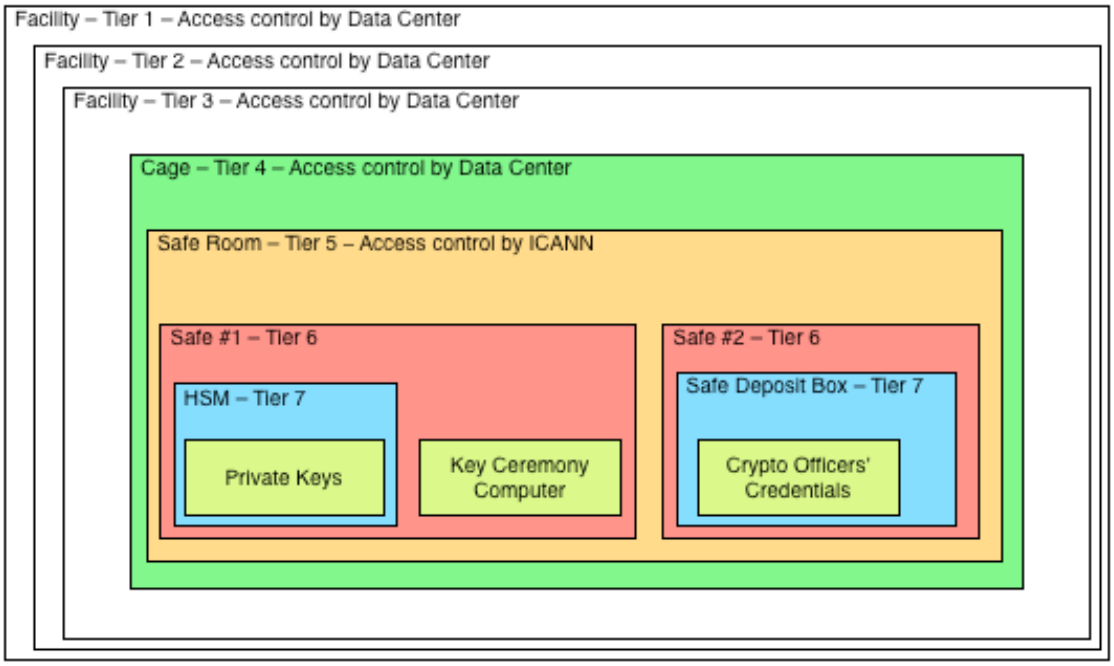

Figure 3

Referring to Figure 3.

The KSKs for the DNSSEC root zone system will be maintained at two offline sites each mirroring the other in functionality. To meet DoC requirements, the two sites maintaining the private half of the KSKs will be geographically dispersed and within the United States: one in Los Angeles, California (near ICANN headquarters) and the other in the metropolitan Washington, D.C. area.

The KSKs will be maintained inside 24x7 manned secure data centers behind multiple tiers of access control. Tiers 1-3 represent various access controls (guard, man-trap, biometrics, etc.) associated with the general secure data center population. Tier 4 represents the key ceremony room and requires biometric access and escort by at least two (2) specifically designated ICANN staff, typically the Ceremony Administrator and Internal Witness. Tier 4 is where HSM initialization, key generation, KSR signing, and key destruction will take place. No equipment executing cryptographic operations will be stored here. Certain data center staff may have access to this tier for maintenance purposes. All entry and exit into Tiers 1-4 will be logged by data center.

Tier 5 cannot be accessed by data center staff and requires two (2) specifically designated ICANN staff. This tier contains two GSA Class 5 safes forming Tier 6. Combinations to each safe are held by two distinct, specifically designated ICANN staff members different from the Ceremony Administrator and Internal Witness.

Safe #1 contains key management software, laptops and the HSMs containing the KSKs. The HSM represents Tier 7 for private key access. There are at least two (2)

HSMs per site holding duplicate key and configurations for backup purposes. HSMs are regularly replaced (destroyed and reinitialized) every five (5) years to ensure functionality and battery life.

Safe #2 contains ten (10) safe deposit boxes (Tier 7) containing the crypto officer smart cards (in tamper evident packaging) needed to activate the HSM. The crypto officers hold the keys to the safe deposit boxes, which adds a layer of protection for the crypto officers from coercion and to the overall system from lost activation data and collusion.

Access to Tiers 5-7 is recorded on log sheets inside the area, safes and in each deposit box as part of audit requirements.

During the key ceremonies, the various cryptographic components are brought into the ceremony room (Tier 4) by those responsible for them and assembled, inserted and executed as needed. Once completed, all material is returned to its original locations. The whole process is filmed from the first entry into Tier 4 until exit.

The ZSK is protected and maintained under similar security conditions.