October 29, 2009

Testing and Implementation Requirements for the Initial Deployment of DNSSEC in the Authoritative Root Zone

Introduction and Baseline Architecture

In recognition of the pressing need for enhanced security for the Internet domain name and addressing system, the Department would like to move forward with its root zone management partners in testing and implementing DNSSEC at the authoritative root zone level, with the goal of a signed root by year-end 2009. To facilitate an accelerated deployment in a secure manner, the Department proposes initially to overlay the deployment process on the existing root zone management process, thereby minimizing the introduction of new steps and changes of responsibilities among the involved parties.[1] The Department envisions the process to include ICANN, the IANA Functions Operator, receiving and processing TLD DNSSEC public key information updates as well as publicly distributing the Root Zone public key; VeriSign, the Root Zone Maintainer, signing the root zone file data and holding the Zone Signing Key (ZSK). Detailed Key Signing Key (KSK) and Zone Signing Key (ZSK) management plans will be jointly developed by ICANN and VeriSign in consultation with the Department.

Meeting this goal will require cooperation and collaboration between the current root zone management partners and the Department, specifically ICANN and VeriSign committing to jointly develop detailed DNSSEC design, testing and implementation plans for the Department to review. The Department sees this arrangement as an interim approach to meet a pressing need with the recognition that advancements in technology and process and/or procedure related to DNSSEC may necessitate change in the future.

General Requirements

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.

The remainder of this section highlights security requirements that should be considered in developing any solution. ISO 27002:2005 (formerly ISO 17799:2005) and NIST SP 800-53 are recognized sources for specific controls. Note that reference to SP 800-53 is used as a convenient means of specifying a set of technical security requirements.[2] It is expected that the systems referenced in this document would meet all the SP 800-53 technical security controls

[1] The Department's current agreements with ICANN (IANA Functions Operator) and VeriSign (Root Zone Maintainer) set forth the root zone management process as: (1) TLD operator submits change request to the IANA Functions Operator; (2) the IANA Functions Operator processes the request; (3) the IANA Functions Operator sends a request to the Department (Administrator) for verification/authorization; (4) the Administrator sends verification/authorization to the Root Zone Maintainer to make the change; (5) the Root Zone Maintainer edits and generates the new root zone file; and (6) the Root Zone Maintainer distributes the new root zone file to the 13 root server operators.

[2] 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.

required by a HIGH IMPACT system.[3]

Whenever possible, references to NIST publications are given as a source for further information. These Special Publications (SP) and FIPS documents are **not** intended as a future auditing checklist, but as non-binding guidelines and recommendations to establish a viable IT security policy. **ICANN and VeriSign may choose to substitute comparable security standards where available and appropriate.** All of the NIST document references can be found on the NIST Computer Security Research Center webpage (http://www.csrc.nist.gov/).

1) Security Authorization and Management Policy

a) Each partner[4] in the Root Zone Signing process shall have a security policy in place; this security policy should be periodically reviewed and updated, as appropriate.

   i) Supplemental guidance on generating a Security Authorization Policy may be found in NIST SP 800-37.

b) These policies shall have a contingency plan component to account for disaster recovery (both man-made and natural disasters).

   i) Supplemental guidance on contingency planning may be found in SP 800-34.

c) These policies shall address Incident Response detection, handling and reporting (see 4 below).

   i) Supplemental guidance on incident response handling may be found in NIST SP 800-61.

2) IT Access Control

a) There shall be an IT access control policy in place for each of the key management functions and it shall be enforced.

   i) This includes both access to hardware/software components and storage media as well as ability to perform process operations.
   ii) Supplemental guidance on access control policies may be found in NIST SP 800-12.

b) Users without authentication shall not perform any action in key management.

c) In the absence of a compelling operational requirement, remote access to any cryptographic component in the system (e.g. HSM) is not permitted.[5]

[3] 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.
[4] For this document, the roles in the Root Zone Signing process are those associated with the Key Signing Key holder, the Zone Signing Key holder, Public Key Distributor, and others to be conducted by the IANA Functions Operator and the Root Zone Maintainer.
[5] Remote access is any access where a user or information system communicates through a non-organization

3) Security Training

a) All personnel participating in the Root Zone Signing process shall have adequate IT security training.

i) Supplemental guidance on establishing a security awareness training program may be found in NIST SP 800-50.

4) Audit and Accountability Procedures

a) The organization associated with each role shall develop, disseminate, and periodically review/update: (1) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

i) Supplemental guidance on auditing and accountability policies may be found in NIST SP 800-12.

ii) Specific auditing events include the following:
- Generation of keys
- Generation of signatures
- Exporting of public key material
- Receipt and validation of public key material (i.e., from the ZSK holder or from TLDs)
- System configuration changes
- Maintenance and/or system updates
- Incident response handling
- Other events as appropriate

b) Incident handling for physical and exceptional cyber attacks[6] shall include reporting to the Department's National Telecommunications and Information Administration (NTIA) in a timeframe and format as mutually agreed by the Department, ICANN, and VeriSign.

c) The auditing procedures shall include monthly reporting to NTIA.

d) The auditing system shall be capable of producing reports on an ad-hoc basis.

e) A version of these reports should be made publically available.

5) Physical Protection Requirements

a) There shall be physical access controls in place to only allow access to hardware components and media to authorized personnel.

---

controlled network (e.g., the Internet).

[6] Non-exceptional events are to be included in monthly reporting as required in 4 c.

i) Supplemental guidance on token based access may be found in NIST SP 800-73 and FIPS 201.
ii) Supplemental guidance on token based access biometric controls may be found in NIST SP 800-76.

b) Physical access shall be monitored, logged, and registered for all users and visitors.

c) All hardware components used to store keying material or generate signatures shall have short-term backup emergency power connections in case of site power outage. (*See,* SP 800-53r3)

d) All organizations shall have appropriate protection measures in place to prevent physical damage to facilities as appropriate.

6) All Components

a) All commercial off the shelf hardware and software components should have an established maintenance and update procedure in place.

i) Supplemental guidance on establishing an upgrading policy for an organization may be found in NIST SP 800-40.

b) All hardware and software components provide a means to detect and protect against unauthorized modifications/updates/patching.

Role Specific Requirements

7) Root Zone Key Signing Key (KSK) Holder

The Root Zone KSK Holder (RZ KSK) is responsible for (1) generating and protecting the private component of the RZ KSK(s); (2) securely exporting or importing any public key components, should this be required (3) authenticating and validating the public portion of the RZ Zone Signing Key (RZ ZSK); and (4) signing the Root Zone's DNSKEY record (ZSK/KSK).

a) Cryptographic Requirements

i) The RZ KSK key pair shall be an RSA key pair, with a modulus of at least 2048 bits.
ii) RSA key generation shall meet the requirements specified in FIPS 186-3.[7] In particular, key pair generation shall meet the FIPS 186-3 requirements for exponent size and primality testing.
iii) The RZ KSK private key(s) shall be generated and stored on a FIPS 140-2 validated hardware cryptographic module (HSM)[8], validated at Level 4 overall.[9]

[7] Note that FIPS 186-3 and FIPS 140-2 are referenced as requirements in sections a and b, rather than supplemental guidance.
[8] FIPS 140 defines hardware cryptographic modules, but this specification will use the more common HSM

iv) RZ KSK Digital Signatures shall be generated using SHA-1 or SHA-256. [10]
v) All cryptographic functions involving the private component of the KSK shall be performed within the HSM; that is, the private component shall only be exported from the HSM with the appropriate controls (FIPS 140-2) for purposes of key backup.

b) Multi-Party Control

At least two persons shall be required to activate or access any cryptographic module that contains the complete RZ KSK private signing key.

i) The RZ KSK private key(s) shall be backed up and stored under at least two-person control. Backup copies shall be stored on FIPS 140-2 compliant HSM, validated at Level 4 overall, or shall be generated using m of n threshold scheme and distributed to organizationally separate parties.
ii) Backup copies stored on HSMs shall be maintained in different physical locations[11], with physical and procedural controls commensurate to that of the operational system.
iii) In the case of threshold secret sharing, key shares shall be physically secured by each of the parties.
iv) In all cases, the names of the parties participating in multi-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

c) Root Zone KSK Rollover

i) Scheduled rollover of the RZ KSK shall be performed.[12] (See Contingency planning for unscheduled rollover.)
ii) RZ KSK rollover procedures shall take into consideration the potential future need for algorithm rollover.
iii) DNSSEC users shall be able to authenticate the source and integrity of the new RZ KSK using the previously trusted RZ KSK's public key.

d) Contingency Planning

i) Procedures for recovering from primary physical facility failures (e.g., fire or flood that renders the primary site inoperable) shall be designed to reconstitute capabilities within 48 hours.
ii) Procedures for emergency rollover of the RZ KSK shall be designed to achieve key rollover and publication within 48 hours. These procedures, which are understood to

---

(for hardware security module) as the abbreviation.
[9] Note that FIPS 186-3 and FIPS 140-2 are referenced as requirements in sections a and b, rather than supplemental guidance.
[10] Utilization of the SHA-2 family is expected once technically feasible / widely available.
[11] Backup locations are to be within the United States.
[12] The Department envisions the timeline for scheduled rollover of the RZ KSK to be jointly developed and proposed by ICANN and VeriSign, based on consultation and input from the affected parties (e.g. root server operators, large-scale resolver operators, etc). Note that subsequent test plans may specify more or less frequent RZ KSK rollover to ensure adequate testing.

address DNSSEC key provision only, should accommodate the following scenarios:
(1) The current RZ KSK has been compromised; and
(2) The current RZ KSK is unavailable, but is not believed to be compromised.

e) DNS Record Generation/Supporting RZ ZSK rollover

i) The RZ KSK Holder shall authenticate the source and integrity of RZ ZSK public key material
   (1) Mechanisms should support proof of possession and verify the parameters (i.e., the RSA exponent)
ii) The signature on the root zone's DNSKEY record shall be generated using SHA-1 or SHA-256.[13]

f) Audit Generation and Review Procedures

i) Designated Audit personnel may not participate in the multi-person control for the RZ ZSK or RZ KSK.
ii) Audit logs shall be backed up offsite at least monthly.
iii) Audit logs (whether onsite or offsite) shall be protected from modification or deletion.
iv) Audit logs shall be made available upon request for Department review.

8) RZ KSK Public Key Distribution

a) The RZ KSK public key(s) shall be distributed in a secure fashion to preclude substitution attacks.

b) Each mechanism used to distribute the RZ KSK public key(s) shall either

i) Establish proof of possession of the RZ KSK private key (for public key distribution); or
ii) Establish proof of possession of the previous RZ KSK private key (for Root zone key rollover).

9) RZ Zone Signing Key (RZ ZSK) Holder

The Root Zone ZSK Holder (RZ ZSK) is responsible for (1) generating and protecting the private component of the RZ ZSK(s); (2) securely exporting or importing any public key components, should this be required and (3) generating and signing Zone File Data in accordance to the DNSSEC specifications.

a) Cryptographic Requirements

i) The RZ ZSK key pair shall be an RSA key pair, with a modulus of at least 1024

[13] Utilization of the SHA-2 family is expected once technically feasible / widely available.

bits.[14]

ii) RSA key generation shall meet the requirements specified in FIPS 186-3.[15] In particular, key pair generation shall meet the FIPS 186-3 requirements for exponent size and primality testing.

iii) RZ ZSK Digital Signatures shall be generated using SHA-1 or SHA-256.

iv) The RZ ZSK private key(s) shall be generated and stored on a FIPS 140-2 compliant HSM. At a minimum, the HSM shall be validated at Level 4 overall.

v) All cryptographic functions involving the private component of the RZ ZSK shall be performed within the HSM; that is, the private component shall not be exported from the HSM except for purposes of key backup.

b) Multi-Party Control

i) Activation of the RZ ZSK shall require at least two-person control. This requirement may be satisfied through a combination of physical and technical controls.

ii) If the RZ ZSK private key(s) are backed up, they shall be backed up and stored under at least two-person control. Backup copies shall be stored on FIPS 140-2 validated HSM, validated at Level 4 overall.[16]

(1) Backup copies shall be maintained both onsite and offsite[17], with physical and procedural controls commensurate to that of the operational system.

(2) The names of the parties participating in multi-person control shall be maintained on a list and made available for inspection during compliance audits.

c) Contingency Planning

i) Procedures for recovery from failure of the operational HSM containing the RZ ZSK shall be designed to re-establish the capability to sign the zone within 2 hours.

ii) Procedures for emergency rollover of the RZ ZSK shall be designed to achieve key rollover within a technically feasible timeframe as mutually agreed among the Department, VeriSign, and ICANN. These procedures should accommodate the following scenarios:

(1) The current RZ ZSK has been compromised; and

(2) The current RZ ZSK is unavailable (e.g. destroyed), but is not believed to be compromised.

d) Root Zone ZSK Rollover

i) The RZ ZSK shall be rolled over every six months at a minimum.[18]

---

[14] Note that these requirements correspond to those articulated in NIST SP 800-78 for authentication keys. Since there is no forward security requirement for the DNSSEC signed data, the more stringent requirements imposed on long term digital signatures do not apply.

[15] Note that FIPS 186-3 and FIPS 140-2 are referenced as requirements in sections 8a and 8 b, rather than as supplemental guidance.

[16] Note that FIPS 186-3 and FIPS 140-2 are referenced as requirements in sections 8a and 8 b, rather than as supplemental guidance.

[17] The Department expects backup locations to be within the United States.

[18] The timelines specified in this document apply to the operational system. Subsequent test plans may

ii) DNSSEC users shall be able to authenticate the source and integrity of the new RZ ZSK using the previously trusted RZ ZSK's public key.
iii) RZ KSK holder shall be able to authenticate the source and integrity of the new RZ ZSK.

e) Audit Generation and Review Procedures

i) Designated Audit personnel may not participate in the control for the RZ ZSK or RZ KSK.
ii) Audit logs shall be backed up offsite at least monthly.
iii) Audit logs (whether onsite or offsite) shall be protected from unauthorized access, modification, or deletion.
iv) Audit logs shall be made available upon request for NTIA review.

Other Requirements

10) Transition Planning

a) ICANN and VeriSign shall develop plans for transitioning the responsibilities for each role while maintaining continuity and security of operations. In the event ICANN or VeriSign are no longer capable of fulfilling their DNSSEC related roles and responsibilities (due to bankruptcy, permanent loss of facilities, etc.) or in the event the Department selects a successor, that party shall ensure an orderly transition of their DNSSEC roles and responsibilities in cooperation with the Department.

11) Personnel Security Requirements

a) Separation of Duties

i) Personnel holding a role in the multi-party access to the RZ KSK may not hold a role in the multi-party access to the RZ ZSK, or vice versa.
ii) Designated Audit personnel may not participate in the multi-person control for the RZ ZSK or KSK.
iii) Audit Personnel shall be assigned to audit the RZ KSK Holder or the RZ ZSK Holder, but not both.

b) Security Training

i) All personnel with access to any cryptographic component used with the Root Zone Signing process shall have adequate training for all expected duties.

12) Root Zone Maintainer (VeriSign) Basic Requirements

a) Ability to receive NTIA authorized TLD Resource Record Set (RRset) updates from

---

specify more or less frequent RZ ZSK rollover to ensure adequate testing.

NTIA and IANA Functions Operator
b) Ability to integrate TLD RRset updates into the final zone file
c) Ability to accept NTIA authorized signed RZ keyset(s)[19] and integrate those RRsets into the final zone file

13) IANA Functions Operator (ICANN) TLD Interface Basic Functionality

a) Ability to accept and process TLD DS records. New functionality includes:

   i) Accept TLD DS RRs
      (1) Retrieve TLD DNSKEY record from the TLD, and perform parameter checking for the TLD keys, including verify that the DS RR has been correctly generated using the specified hash algorithm.
   ii) Develop with, and communicate to, TLD operators procedures for:
      (1) Scheduled roll over for TLD key material
      (2) Supporting emergency key roll over for TLD key material.
      (3) Moving TLD from signed to unsigned in the root zone.

b) Ability to submit TLD DS record updates to NTIA for authorization and subsequent inclusion into the root zone by the Root Zone Maintainer.
c) Ability to submit RZ keyset to NTIA for authorization and subsequent inclusion into the root zone by the Root Zone Maintainer.

14) Root Zone Management Requirements[20]

a) Ability and process to store TLD delegations and DS RRs
b) Ability and process to store multiple keys for a delegation with possibly different algorithms
c) Ability and process to maintain a history of DS records used by each delegation
d) Procedures for managing scheduled roll over for TLD key material
e) Procedures for managing emergency key roll over for TLD key material.[21]
f) Procedures for managing the movement of TLD from signed to unsigned.[22]
g) Procedures for DNSSEC revocation at the root zone and returning the root zone to its pre-signed state.

[19] Dependent on how ICANN and VeriSign propose KSK management, the Root Zone Maintainer (VeriSign) may need to consider the ability to accept the signed RZ key set from an outside party.
[20] The Department envisions ICANN and VeriSign jointly deciding and proposing how each of these requirements are to be designed and implemented, subject to Department approval.
[21] To the extent possible, on 24 hour notice under the existing manual system and on 12 hours notice once the automated system is utilized.
[22] To the extent possible, this should be within 48 hours.