VeriSign

September 22, 2008

Ms. Meredith A. Baker
Acting Assistant Secretary for Communications and Information
United States Department of Commerce
National Telecommunications and Information Administration
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: DNSSEC

Dear Ms. Baker:

On September 16, 2008, representatives of VeriSign and ICANN met to discuss proposals for signing the DNS root zone with the DNS security extensions known as DNSSEC. At the meeting, the parties discussed ICANN's recent proposal to the Department of Commerce for DNSSEC as well as an alternative plan developed by VeriSign. At the conclusion of the meeting, VeriSign advised ICANN that it would submit its proposed plan for DNSSEC to the Department of Commerce.

Accordingly, the attached proposal is being presented to the Department of Commerce and ICANN for the purpose of reviewing technically responsible approaches to DNSSEC. VeriSign is committed to signing the root zone within the next 12 months and the .com and .net gtld zones within the next 18 to 24 months, with the expectation that the current outstanding technical issues around DNSSEC will be resolved.

As you are aware, VeriSign is currently sponsoring a test bed for DNSSEC signing of the root. We look forward to working with the Department of Commerce, ICANN and the root server community to find the most expedient and acceptable path forward to ultimate DNSSEC enablement of the root. We welcome your comments and suggestions regarding this proposal. We are also sharing this proposal with interested parties and working groups in the community so that this proposal can be vetted alongside other proposals.

We look forward to discussing this proposal with you at your convenience.

Best Regards,

Kenneth J. Silva, Jr.
Chief Technology Officer

cc: ICANN

Root Zone Signing Proposal

22 September 2008

Executive Summary

This document describes VeriSign's proposal for signing the DNS root zone with the DNS Security extensions known as DNSSEC. This proposal is being presented to the Department of Commerce (DoC) and ICANN for the purpose of developing a joint approach to DNSSEC in accordance with the terms of the Root Server Management Transition Completion Agreement between VeriSign and ICANN.

What this proposal does

- **Uses existing roles to reduce complexity and confusion.** In accordance with DoC NTIA's previously stated public position, the existing roles of ICANN, VeriSign and the Department of Commerce are preserved. In particular, VeriSign continues to both generate and distribute the root zone.

- **Deploys the Root Zone Management System as announced and planned.** ICANN and VeriSign would work together to deploy the Root Zone Management System (RZMS) as previously announced to DoC. ICANN and VeriSign would continue to work together on RZMS to add support for DNSSEC, allowing ICANN to provision DNSSEC key material for top-level domains (TLDs) in the root zone.

- **Splits control of the root zone key-signing key (KSK).** Rather than being assigned to the care of a single organization, control of the root zone KSK is split among multiple entities.

- **Addresses the international community's concerns over KSK control.** The existing root operators, a technically competent and neutral group of organizations with international representation, would share control of the root zone KSK. Because the root operators do not possess the necessary infrastructure to securely store and use this key, certain key-handling responsibilities would realistically need to be contracted to a third party. VeriSign has the necessary experience, facilities and processes and would be available to handle these responsibilities.

- **Uses existing and proven resources and processes.** The role of the root zone maintainer would be expanded to include root zone signing. The root zone maintainer would also generate the root zone zone-signing key (ZSK) as necessary. VeriSign, as the current root zone maintainer, already has significant experience, secure facilities and mature processes to assume the additional signing responsibilities.

- **Follows industry standard and internationally recognized public key infrastructure (PKI) processes.** All key material would be stored securely in FIPS 140-2-compliant hardware security modules (HSM). All key creation and signing would take place in secure facilities and follow documented processes, all in accordance with industry best practices. All activities would be transparent and subject to third-party audits.

- **Calls for significant testing to understand the impact and reduce risk.** The root zone would be signed as soon as all parties can be ready, but not before an extensive test bed is established to observe the effect of a signed root zone in widespread use. The existing root operators would run this test bed on separate servers dedicated to this purpose.

What this proposal does not do

- **Preclude any changes in roles or responsibilities at a later date.** The solution described in the proposal could be implemented without precluding changes in roles or responsibilities in response to further developments.

- **Force changes to existing roles and responsibilities prematurely.** The current root management process is stable and successful. Each of the three parties (ICANN, as IANA functions contract holder; VeriSign, as root zone maintainer; and DoC, as root zone change authorizer) perform a role suited to their respective strengths and capabilities. Signing the root zone need not, and should not, change these roles prematurely and unnecessarily, which has potential to weaken the stability of the overall root management process.

- **Require any changes to top-level domain behavior.** Signing the root does not require every TLD to take any specific action. Only those TLDs that wish to sign their zone need to perform the extra step of submitting their zone's key material to ICANN for publication in the root zone.

Goals

It is helpful when reading this proposal to understand the goals for a signed root zone that VeriSign followed in its preparation.

- **Preserve existing roles and responsibilities.** In accordance with DoC NTIA's previously stated public position, this proposal does not change any of the roles and responsibilities of the three parties that currently cooperate to perform the root zone change process:

- ICANN, under the IANA functions contract, continues to accept and validate requests from TLD managers and submit the requests to NTIA for authorization and VeriSign for implementation.
- VeriSign continues to implement these changes to produce the authoritative root zone file and publish these changes to the root operators.
- NTIA continues its role in authorizing changes to the root zone.

- **Sign the root expeditiously but cautiously.** The root should be signed without undue delay, but we recognize that this operation is a significant undertaking, requiring the coordination of several parties, and will therefore take time. Further, the root zone is the most important zone in DNS and also one of the most queried zones. Its stability is vital, as is the stability and proper operation of clients that query the root zone. Signing the root cannot disrupt root operations (producing, publishing and serving the root zone), nor especially can signing the root disrupt DNS resolution throughout the Internet. The root zone is queried by literally millions of DNS clients and signing the root cannot be allowed to break resolution of even a small percentage. Proper testing in advance of signing the production root is therefore important to gauge the impact. Any decision to sign must include a review of the testing results to determine what actions, if any, may be needed to ease any harmful effects of signing the root before proceeding.

- **Split control of the root zone key-signing key.** When discussion of root signing occurs, the question of what organization will control the root zone KSK inevitably emerges as a complicated and contested issue, with different parties expressing different positions, sometimes in complete opposition. Determining control of the KSK is a significant issue because of the importance of this key: from a technical perspective, whoever controls it is the final authority over what information is published in the root zone.

  A well-established technique used in the public key infrastructure industry offers another option to simplify this control issue: rather than being controlled by a single organization, control of the KSK can be split among multiple organizations. In this model, multiple organizations must cooperate to create and use the key. For such an important function as the root zone KSK, requiring multiple parties is a better alternative than vesting control in a single organization, which is subject to failure or capture by other parties desiring control of the root zone.

- **Allow appropriate parties to control the root zone KSK.** Splitting control of the KSK allows multiple parties to authorize its use, but these parties must be chosen with care. The parties must be:
    - Neutral, without a stake in the contents of the root zone;
    - Trustworthy, with an established and public record;
    - Non-controversial, likely to be accepted by a large portion of the Internet community, including the international community; and
    - Competent, with an understanding of DNSSEC, an appreciation of operational matters, and the capabilities to perform this role in a secure manner (potentially subcontracting certain responsibilities, such as physical key storage, as necessary).
- **Store and use all root zone keys securely.** The root zone keys (both KSK and ZSK) will be extremely sensitive and need extraordinary protection. A compromised ZSK would allow forged signatures of root zone data, and the KSK will be configured as a "trust anchor" in millions of DNSSEC validators; its loss would require an unprecedented amount of reconfiguration across the entire Internet to update trust anchors and the potential exposure resulting from its loss is significant.

Key Elements of the Proposal

Figure 1 provides a graphical overview of the proposed root zone management process with zone signing added that is described in the following sections.

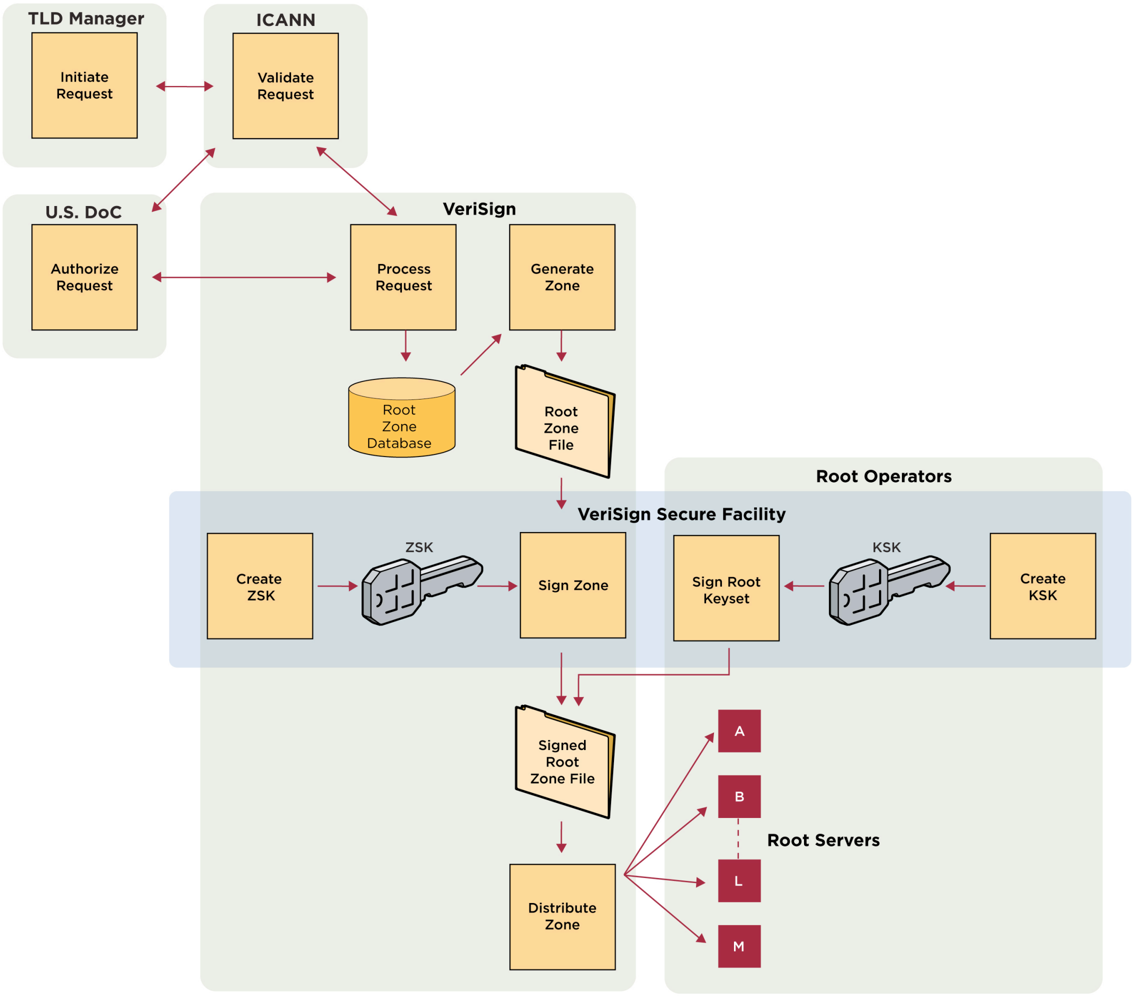

Figure 1: Root zone management process overview (proposed)

1. *Key handling practices*

The importance of the KSK and ZSK will require extraordinary levels of protection for these keys. Before we describe the specific aspects of signing the root zone, we describe the means that will be necessary to protect the keys used to sign the zone.

1.1. Hardware Security Module

All root zone keys (both KSK and ZSK) must be stored in a hardware security module (HSM), a device that allows a key to be used for signing without exposing the key for compromise by storing its private portion in tamper-resistant hardware. An HSM can be considered conceptually as a "black box" that securely creates and stores a private key and then uses that key to sign data sent to it.

A description of a particular HSM will be helpful to understand the concept. This example is based on the hardware used by VeriSign for both its SSL certificate operations and its DNSSEC signed root test bed, but any HSM with the same level of security will be similar. With this HSM, a public/private key pair is created and stored on a removable security "token", roughly the size of a cassette tape. Not only does the token contain storage for the private portion of the key, but the token also has limited processing power to perform digital signing operations using the private key. Thus the private key does not need to leave the token for signing. In fact, by design, the private key cannot be extracted or exported to be used elsewhere, except to create a copy of the token (see below). The physical token hardware is tamper-resistant to make it extremely difficult to extract the private key even with physical possession of the token. Indeed, the main reason for using an HSM is this secure storage of the private key.

The token fits into a chassis, which has an interface to connect to an external device, such as a computer. This interface allows the HSM to receive unsigned data, which is sent to the token for signing, and to send the signed data back out to the external device.

The chassis has slots for two tokens to be inserted simultaneously, which allows tokens to be copied or "cloned". During this operation, the private key is encrypted and this encrypted copy of the key briefly traverses the backplane of the chassis as it is copied from the original token to the copy. (Thus at no point during the lifetime of a token is the private key ever exposed in unencrypted form outside the token.) Having a copy of a token is necessary to protect against damage or loss of the original, and also allows a copy to be kept in a backup facility for disaster recovery (DR) purposes.

1.2. Secure facilities

Using an HSM for private key storage and signing is only a small part of a comprehensive solution. Tamper-resistant hardware is not tamper-proof, so the HSM must be stored in a secure facility with strict, multi-tiered access controls. A typical enterprise data center would not be sufficient, nor would a shared facility such as a commercial hosting or co-location facility. For example, VeriSign's HSMs and other systems supporting its SSL certificate and DNSSEC test bed operations are placed in a "Tier 4" facility. This designation means that they are operated in an environment where there are four physical separation and validation points that must be passed to access to the equipment. VeriSign's standard is to use dual methods of biometric authentication as well, including hand geometry and retina scans, to access the data center facility housing the sensitive HSM equipment.

These facilities must be subject to third-party audit. For example, VeriSign's data centers housing its SSL certificate and DNSSEC test bed operations receive a periodic Statement on Auditing Standards (SAS) number 70 (Service Organizations) Type II audit. This rigorous audit process is an industry-recognized procedure developed by the American Institute of Certified Public Accountants (AICPA).

1.3. Comprehensive policies and documentation

Finally, secured equipment in a secure facility is useless without careful, thorough and well-documented policies governing its use. Significant policy development and corresponding detailed documentation will be required to describe all aspects of root zone key usage and signing. The level of sensitivity and importance of root zone key material is comparable to the sensitivity and importance of SSL Certificate Authority (CA) root keys, which ultimately sign all certificates issued by that CA. Thus it would be reasonable to expect that the size and scope of documentation needed to adequately document the policies for using DNSSEC root zone keys would be comparable to the documentation governing the operation of an SSL CA. By way of comparison, VeriSign's latest Certification Practice Statement (CPS)[1], which covers every aspect of its certificate issuance operations, is 118 pages long.

[1] VeriSign's latest CPS is found at *http://www.verisign.com/repository/CPSv3.8_final.pdf*.

2. *Root zone signing*

2.1. Root zone maintainer signs the root zone

Since a goal of this proposal is to preserve existing roles and responsibilities, and since the root zone maintainer is currently VeriSign, it follows that VeriSign should sign the root zone. This decision makes sense operationally: the zone maintainer generates and distributes the root zone, and zone signing obviously needs to occur after the zone is generated but before distribution. If the zone maintainer did not sign the root zone, it would require sending the root zone file to some other organization for signing and then retrieving the signed version for distribution. These additional steps would introduce the possibility of data manipulation, data corruption or delay into the root zone management process.

VeriSign's undertaking the zone signing responsibility preserves its current role in the overall root management process.

2.2. Root zone maintainer creates the root zone ZSK

The root zone is currently generated twice daily and would therefore need to be signed twice daily with the root zone's ZSK. Since the root zone maintainer (VeriSign) would be using root zone ZSK on a daily basis to sign the zone, we propose that VeriSign also be responsible for creating a new root zone ZSK, as necessary. This choice makes sense based on the secure nature of an HSM, which as described above does not allow the private portion of any keys it stores to be extracted or exported.

The alternative to the root zone maintainer's creating a new ZSK would be for some other organization to create the key, but this choice is problematic operationally. Since a key can only be created in an HSM[2], requiring physical possession of the HSM, the HSM hardware containing the private portion of a newly created ZSK would have be physically transported from where it was created to the zone maintainer's (VeriSign's) facility to be used for signing. Moving the hardware containing the private key would have to be accomplished securely and introduces logistical complexity and potential delay, the possibility of key compromise and added expense.

Having the root zone maintainer creating root zone the ZSK should be non-controversial. VeriSign, as the current maintainer, has the facilities, processes and

[2] Or, in the case of the particular HSM used by VeriSign, a removable tamper-resistant hardware token that fits into an HSM chassis.

experience to perform this key creation securely. Further, it is important to keep in mind that by design, a root zone ZSK will be shorter-lived than the root zone's KSK, and the ZSK derives its legitimacy from being signed by the KSK. Any concerns over control of the root zone via DNSSEC should focus on control of the KSK, not the ZSK.

3. KSK control and use

3.1. Split control of root zone KSK

We propose to split control of the KSK among multiple organizations using the "M-of-N" technique, which is a PKI industry standard practice that is supported by various Hardware Security Modules, including the specific one used by VeriSign. In this technique:

- **N** is the number of entities that share control of the key, and,
- **M** is the minimum number of those entities that must agree to any use of the key, e.g., using it for signing.

Splitting control of the KSK avoids the various issues associated with vesting complete power over the key in any single organization.

To aid in understanding the concept, it is helpful to describe how the technique is actually implemented in the HSM used by VeriSign. Recall that the private key material is stored on a small token that fits into the HSM chassis, which allows connectivity to an external device for accepting unsigned data and returning signed data. Connected to this chassis is a number pad with a slot for a plastic key supplied by the manufacturer to be inserted. Each plastic key has a chip embedded in it with an electronic serial number that identifies the specific plastic key to the HSM. (Note that no private key material is stored on the plastic key: the plastic key is only an identifier.) A personal identification number (PIN) is also associated with each plastic key to provide two-factor authentication: possession of a plastic key alone is not sufficient to authenticate to the HSM. The plastic key-holder must also know that key's PIN.

Different plastic keys are required to authorize the HSM to perform different functions. An operator inserts a plastic key into the number pad and types that key's PIN to authenticate to the HSM and enable a particular function. The manufacturer codes the plastic keys different colors according to their function. Green keys are used to support the M-of-N functionality.

When a token is initialized for the first time, up to 16 green keys can be associated with it. Each entity with a stake in controlling the private key stored on the token is given a green key. In other words, the number of green keys is the value **N** in M-of-N. At the time of token initialization, the number of green keys that must be present to authorize the token's use must also be specified. This number represents the value **M** in M-of-N. Once a token is initialized with the M-of-N scheme, any private keys created on it will require M-of-N green keys to be physically present for those keys on the token to be used for signing. At least M green keys must be inserted into the number pad, one at a time, and the corresponding PIN entered by the key's owner, to enable the HSM to perform signing operators. This requirement applies to all copies of the token, as well.

3.2. Root operators control KSK

Since the M-of-N technique allows control of the KSK to be split, an acceptable group of organizations must be found among which to divide control of the key. We propose that the current twelve root operator organizations are an ideal choice to control the root zone KSK. This choice has several advantages.

The root operators represent widely varied types of organizations: commercial, non-profit and educational. Three of the twelve organizations are based outside the United States, providing international representation. This group has a long history, with some root operators having served over 15 years. Historically the group has been singularly focused on serving the root zone administered by the IANA function, with no other political interests. The group has an established record of successful service to the Internet community. By having had no purpose other than successful root zone service, the root operators are actually excellent candidates to be custodians of the root zone KSK: KSK creation and use is just another technical task for a group that has already demonstrated its technical competence.

While the root operators as a group are qualified to make the responsible administrative decisions necessary to control the KSK, handling the sensitive cryptographic material of a KSK would require additional facilities and processes that the root operators as a group do not possess. However, these functions could be contracted to a third party. VeriSign proposes that it could handle these functions at the behest of the root operators. Note that acting in this subcontractor role would not give VeriSign any special control over the KSK. Rather, VeriSign could apply its secure facilities and expertise to allow the root KSK to be used and stored securely.

More specific details describing how the root operators would administer the KSK using the M-of-N technique are found below in the section entitled *Operational Considerations*.

4. Testing

4.1. Test bed before production

No zone as important or as widely queried as the root has yet been signed. The largest zones yet signed are some smaller TLD zones and while deployment has gone reasonably smoothly, the process has not been completely without incident. Because of the critical nature of the root zone, and because it is so widely queried, we can expect the sort of issues discovered during smaller initial DNSSEC deployments to be magnified when the root is signed. As a result, it is vital that any plan to sign the root include an initial testing phase. Any other rush to full-scale signing of the root would be operationally irresponsible.

We propose a test bed phase in which a signed version of the authoritative root zone is widely available for interested parties to test against. To be successful, this test bed needs to be heavily used by a diverse set of clients. To achieve significant use, the test bed must be widely publicized so DNS administrators throughout the Internet are aware of its existence. Further, the test bed must be run in a manner that instills confidence so administrators are willing to trust some amount of production DNS resolution traffic to it.

Test infrastructure tends to remain active indefinitely and slowly slip from test mode to *de facto* production if the testing is not strictly managed. The test bed needs a firm ending date and this information must be communicated clearly and widely at the beginning of the exercise and continually throughout, so that there can be no uncertainty or surprises about the duration of the test.

Setting up a test bed for a finite duration and encouraging its use is not sufficient. The exercise requires goals and evaluation criteria, which need to be clearly documented. The test bed itself needs to be instrumented to determine the nature of traffic it receives (number of clients, kind of queries sent, etc.). There must be an easy mechanism for users to provide feedback on their experiences. All information gathered must be analyzed and documented at the test bed's end so any actions necessary before proceeding with signing the root in a production capacity can be undertaken.

4.2. Root operators run test bed

The existing root operators would be a logical choice to run a signed root test bed. They are already trusted to publish the production root zone, so any test they also provided would have a large measure of credibility. The root operators also have the operational experience to run such a test bed and some have already expressed interest in deploying the additional infrastructure to support it. VeriSign has suggested such a test bed already and there is interest among some of the operators. Not all operators would need to participate: a subset could still provide more than enough capacity for an effective test bed.

The test bed described here would uses the authoritative root zone as its basis and the official root operators would serve it, so the Department of Commerce may decide that its authorization is required. This authorization would be helpful to legitimize the test bed and help reduce the perception that it in any way represents an "alternate root". Rather, the test bed would represent an official version or extension of the official root zone, for the first time offered in a test capacity. More specific details about the implementation of this test bed are found below in the section entitled *Operational Considerations*.

5. Root Zone Management System

5.1. Finish currently planned deployment

VeriSign and ICANN have been working together on a project called the Root Zone Management System to improve the root zone editing and publishing infrastructure. ICANN's portion includes new "eIANA" software that offers a web-based interface to TLD managers to submit changes, improving the existing email template interface used by TLD managers to submit changes today. VeriSign's portion includes a new registry system dedicated to the root zone with a workflow system to track root zone changes and automate certain tasks. Together, VeriSign and ICANN have implemented a new mechanism to communicate root zone changes from ICANN to VeriSign. Rather than relying on email templates, the new system uses the Extensible Provisioning Protocol (EPP) to efficiently and unambiguously communicate change requests.

VeriSign and ICANN verbally briefed the Department of Commerce on this system in May, 2008, and left that meeting with the action to submit a written proposal for official consideration by the Department, which would need to authorize the system's deployment. VeriSign and ICANN have been working together to create this proposal, which will call for a prolonged period of parallel operations during which the old and new systems run simultaneously to ensure correct operation of the new system.

This proposal for signing the root zone has no impact on the RZMS proposal. VeriSign and ICANN have invested significantly in the RZMS and its deployment will represent a significant improvement in root zone operations. VeriSign desires to deploy this system as soon as possible and will continue to work with ICANN on RZMS.

5.2. Extend RZMS to support DNSSEC

Once deployed, RZMS will need to be extended to support DNSSEC. A signed root will necessitate that ICANN, under the IANA functions contract, accept DNSSEC key material from TLD managers. This key material corresponds to the public portion of TLD zone KSKs and needs to appear in a signed root zone as Delegation Signer (DS) records. ICANN will need to communicate this key material to VeriSign for publication in the root zone.

VeriSign proposes to begin working with ICANN immediately to plan and implement the changes to the RZMS required by DNSSEC.

Operational Considerations

This section describes some of the operational considerations of this proposal. It elaborates on some of the general proposals described above to give specific examples of how these concepts could actually be implemented.

1. KSK creation and use

While the root operator organizations will control the KSK under this proposal, VeriSign proposes to provide the facilities for secure use and storage of this key since no other operator is qualified with the same level of experience and secure facilities.

The following descriptions provide only an overview. Ultimately these processes will need to be defined in detail and scrupulously documented.

1.1. KSK generation

The root zone KSK should be a long-lived key because mechanisms to change this key, referred to as "rolling" it, are in the early stages of development and not yet widely implemented. Thus we should expect the initial KSK to last for several years and the creation ceremony described below will therefore happen infrequently.

VeriSign's main secure facility is located in Mountain View, California, with two disaster recovery facilities elsewhere. The Mountain View secure facility includes a "key ceremony" room. This room houses an HSM chassis connected to a computer with no network access, so all key operations are confined to the room. All proceedings in the room are videotaped.

For the initial KSK creation, all the root operators that would share control of the KSK would need to send a representative to appear in person to participate in the ceremony. Other parties could also be present to observe and report on the proceedings. Each operator representative would be issued a green plastic key and would choose a PIN for that operator's key. A new HSM token would be inserted into the HSM chassis and initialized for M-of-N authorization. In this case, **N** would be the number of root operator organizations physically present in the room. A reasonable value for **M** would need to be chosen based on N. We suggest (N/2)-1, i.e., one fewer than half the number of operators present. Thus if all 12 operator organizations are able to be present, N would be 12 and M would be 5.

As part of the token initialization, each operator would insert its green plastic key into the HSM number pad and enter the PIN. This sequence of actions establishes the green keys that are now eligible to participate in the M-of-N authentication scheme for this token. Next, the actual KSK would be created on the token. This action will require M-of-N operators to authenticate to the HSM using their green key to authorize key creation. Once created, the public portion of the KSK will be exported to the computer connected to the HSM, from which it will be copied to multiple storage devices (e.g., CD ROMs and USB tokens) and distributed among the assembled participants and observers. The public portion of the root zone KSK will be published in multiple locations as the new root zone trust anchor. This publication will require proper authentication (such as being served from an SSL-protected web page). The new key will be configured as a trust anchor in DNSSEC validators by administrators all over the Internet.

Next the HSM token containing the root zone KSK will be cloned so there are multiple copies for redundancy purposes. At a minimum, sufficient copies will be made for storage at VeriSign's Mountain View and disaster recovery facilities. The copies destined for the disaster recovery facilities will be transported securely by VeriSign personnel, never leaving their personal physical possession. Optionally, further copies of the token could be given to selected root operator representatives, provided that they have the means to securely store the tokens. As a reminder, please recall that all copies of the token require M-of-N authorization for use, so physical possession of a token does not allow the holder to actually use the token without at least M of the other N operators present and willing to authenticate.

With all operators present, they will next proceed to use the just-generated root zone KSK to sign multiple root zone key sets for the upcoming year, as described in the next section.

1.2. Using the KSK to sign root zone key sets

The primary purpose of the root zone KSK is to sign root zone key sets. The root zone key set refers to all DNSKEY resource records (RRs) located at the DNS root node

(“.”). The key set consists of the root zone KSK and all ZSKs in use. In some cases, only one ZSK will be present in the key set, but during a ZSK rollover—the period of transition moving from an old ZSK to a new one—there will be two ZSKs in the key set. The signature of the root key set created using the root zone KSK is included in the root zone itself. (This is the only data signed by the root zone KSK that appears in the root zone.)

The root zone key set needs to be signed at a minimum every time the ZSK changes. From a practical standpoint, however, it should be signed more frequently: DNSSEC best practices call for keeping a zone’s key set’s signature as short as reasonably possible. While exact values still need to be determined and should be based on further research and consultation with cryptographic and DNSSEC experts, for purposes of this proposal, we initially and preliminarily propose that the root zone’s ZSK be used for one year and that the root zone’s key set signature have a lifetime of one month. Thus the same key set would be re-signed twelve times, each time producing a signature valid for just one month.

Since the root zone KSK signs the root key set, it might at first appear that the KSK would need to be used once per month to sign a new key set, which would require the physical presence of M-of-N operators to authorize use of the KSK. This need not be the case and would not be realistic: it would not be possible, nor operationally feasible, to expect M-of-N root operators to come to VeriSign’s Mountain View facility each month. Instead we propose that the root operators meet in Mountain View at the secure key ceremony room once per year. At this meeting, the root operators would authorize use of the KSK to sign the next year’s entire set of key sets (twelve in all) in advance. The root zone maintainer and signer (currently VeriSign) would store these key sets and use them throughout the year as required.

It is important to note that the HSM token containing the KSK’s private key will be stored in a safe in a secure facility for most of its lifetime. The token is only removed from the safe and brought to the key ceremony room when M-of-N root operators are present to use the KSK for signing the root key set. This extreme physical protection is commensurate with the importance and sensitivity of the KSK and helps protect against key compromise.

This proposal allows relatively infrequent physical meetings of the root operators while maintaining the DNSSEC best practice of relatively short key set signature lifetime.

2. Test bed

This section describes additional operational details for the proposed signed root test bed.

2.1. Source of signed zone

VeriSign announced a root zone test bed in March, 2008. The purpose of this project was to finish the necessary development and be ready to sign the root in a production capacity when asked. VeriSign's test bed has been signing the authoritative root zone file for several months in a manner nearly identical to an eventual production signing of the root: the test bed signing process uses the same secure infrastructure and processes as VeriSign's SSL certificate operations. However, the test bed has concentrated on signing, not serving, the root zone and has essentially no resolution component. The signed root zone originating from VeriSign's existing DNSSEC test bed would be an ideal source for a signed root test bed with a resolution component offered by the root operators.

2.2. DS record provisioning

In an eventual production signed root zone, each TLD zone that is signed will require a DS record corresponding to its KSK to be present in the root zone. The TLD manager will send its KSK to ICANN, in its role under the IANA functions contract, and then ICANN will send the KSK to VeriSign, in its role as root zone maintainer, using the EPP interface developed for the RZMS.

For the test bed to be useful, the signed root zone in the test bed needs to include all currently signed TLDs' DS records, as well. However, ICANN is not currently accepting key material from TLDs, so the DS records must be obtained via a different method.

Because the current number of signed TLDs is small, it is possible to implement a manual process. For the signed root zone in our test bed, VeriSign is verifying the authenticity of each signed TLD's KSK by hand. (For example, by consulting an SSL-protected web page published by the TLD listing its key, or making personal contact with TLD administrators to verify their KSK's validity.) This process could be continued for the foreseeable future and allow a useable signed root zone to be published in a test bed operated by the root operators as described earlier in this document.

A possible alternate mechanism for obtaining TLD key material is ICANN's proposed trust anchor repository (TAR). ICANN has indicated its intentions to collect key material from signed TLDs and publish those keys. This collection of TLD keys (really just a file in a standard, machine-parsable format) is called a trust anchor repository. If ICANN’s TAR becomes available, it would be an easier source of TLD key material than the current manual process implemented by VeriSign. We recommend that the test bed signed root use the key material from an ICANN-published TAR if and when it becomes available.