Homeland Security

Signing the Domain Name System Root Zone:

Technical Specification

Prepared for:
Science and Technology Directorate
US Department of Homeland Security

Prepared by:
National Institute of Standards and Technology
SPARTA, Inc.
Shinkuro, Inc.

31 October 2006

Signing The Domain Name System (DNS) Root Zone: Technical Specification

Version 3.0.2
31 October 2006

National Institute of Standards and Technology
SPARTA, Inc.
Shinkuro, Inc.

Document Distribution List

First Name	Last Name	E-mail
Jakob	Schlyter	<jakob@rfc.se>
Geoff	Sisson	<geoff@nominet.org.uk>
Rob	Austein	<sra@hactrn.net>
Peter	Koch	<pk@isoc.de>
Olaf	Kolkman	<olaf@nlnetlabs.nl>
Leslie	Daigle	<leslie@thinkingcat.com>
David	Conrad	<david.conrad@icann.org>
Vinton G.	Cerf	<vint@google.com>
Thomas	Narten	<narten@us.ibm.com>
Russ	Housley	<housley@vigilsec.com>
Steve	Bellovin	<smb@cs.columbia.edu>
John	Biccum	<johnbic@microsoft.com>
Michael	Green	<mgreen@nic.mil>
Matt	Larson	<mlarson@verisign.com>
Jaap	Akkerhuis	<jaap@nlnetlabs.nl>
Mike	St. Johns	<mstjohns@comcast.net>
Patrik	Faltstrom	<paf@cisco.com>
Daniel	Karrenberg	<daniel.karrenberg@ripe.net>
Johan	Ihren	<johani@autonomica.se>
Frederico	Neves	<fneves@registro.br>
Suzanne	Woolf	<Suzanne_Woolf@isc.org>
Piet	Barber	<pbarber@verisign.com>
Brian	Coppola	<bcoppola@verisign.com>
John	Crain	<crain@icann.org>
Karl	Reuss	<reuss@umd.edu>
Mark	Schleifer	<marks@schleifer.org>
Yuji	Sekiya	<sekiya@wide.ad.jp>
Gerry	Sneeringer	<sneeri@umd.edu>
Mike	Corcoran	<mikec@niscc.gov.uk>
Ashley	Cross	<ashley.cross@dcita.gov.au>

This draft is intended for distribution to U.S. Government, designated contractor personnel and specific individuals identified in the Document Distribution List.

Table of Contents

List of Figures

List of Tables

Executive Summary

The Domain Name System (DNS) is a critical infrastructure service for the Internet. This system provides the name to IP addresses translations and vice versa. DNS is one of the most widely used services on the Internet. Because of this ubiquitous presence the accuracy, dependability and availability of the DNS is critical to the ongoing operations of the Internet.

The current Domain Name System protocol has a number of security vulnerabilities. The DNS Security Extensions (DNSSEC) have been defined and developed as the principal means to address some of these protocol security vulnerabilities. Since the Root Zone is at the top of the DNS hierarchy, it should be signed as soon as possible since this will facilitate verifying a chain of trust from the Root Zone Public Key. Any DNS resolver on the Internet that configures the Root Zone Public Key as a Trust Anchor will be able to perform this verification. This document specifies various alternative methods, including software alternatives that can be used to sign the Root Zone.

In order to achieve an operational DNSSEC signed Root Zone, a number of changes need to be made to the existing process that is used for maintaining and changing the content of the Root Zone. This specification focuses exclusively on this aspect of achieving a signed the Root Zone. Additionally, this specification was developed with the intent of minimizing changes to the existing process. When a particular activity could be accomplished in different ways, minimizing changes to the existing processes was the dominant factor in selecting the specific method.

Full operation of DNSSEC at the Root level requires several component capabilities. Both key signing and zone signing keys (KSK and ZSK) need to be generated. The public part of the KSK needs to be distributed to the community and used by resolvers everywhere. The software, hardware, and procedures within the IANA, Root Zone Maintainer, Root Zone Distributor and the root server operators need to be modified to accommodate DNSSEC.

There are two sets of keys that will be used to sign the Root Zone. The first type of key is called the Key Signing Key and the second type of key is called the Zone Signing Key. The private portion of the Key Signing Key (KSK) is used to sign the Root Keyset published in the Root Zone. The KSK public key will be the “Root Zone Public Key” and will be published via various means and configured into security-aware DNS resolvers as a Trust Anchor. The private portion of the Zone Signing Key (ZSK) is used to sign all of the non-key data in the Root Zone. The public portion of this key should never be configured as a Trust Anchor by any DNS resolver.

A significant addition to the existing architecture proposed by this specification is the function of the “Root Key Operator” (RKO). The RKO will be responsible for the generation and use of the root’s Key Signing Key (KSK), which will be the top-level key for the entire DNS hierarchy. Although it is theoretically possible to have multiple RKOs, the operation is much more complex and not recommended. This new function could, in principle, be assigned to a variety of organizations. While the KSK is the top-level key for the DNS hierarchy, the root Zone Signing Key (ZSK) performs the day-to-day signing of the Root Zone. There are three possible architectural options based on where the generation and use of the ZSK takes place. The possible options add five steps to the existing process.

The architectural options are paralleled by a set of technological and operational options for performing the additional steps added to the process. The critical aspect of the technological options is that any cryptographic library used by the options must be FIPS 140-2 Level 3 compliant. The most critical aspect of the operational options is that key rollovers must be smooth and cannot cause any interruption in providing the DNS service.

There are four organizational options for the Root Key Operator: 1) New unit within an existing governmental agency, 2) New unit operated by a contractor (under contract to an existing governmental agency), 3) Existing governmental unit, 4) Existing unit operated by a contractor (under contract to a governmental unit). The RKO’s functions may be understood as: routine operations functions, supervisory and management functions, technology evolution, communications, policy/legal, and finance.

This page intentionally left blank.

1 Introduction

The Domain Name System (DNS) is a critical infrastructure service for the Internet. This system provides the name to IP addresses translations and vice versa. DNS is one of the most widely used services on the Internet. Because of this critical function and its ubiquitous presence the accuracy, dependability and availability of the DNS is critical to the ongoing operations of the Internet.

The current Domain Name System (DNS) protocol has a number of security vulnerabilities. The DNS Security Extensions (DNSSEC) have been defined and developed as the principal means to address some of these protocol security vulnerabilities. The design of DNS and DNSSEC permits each DNS zone to be operated and signed independently from other DNS zones. As a result, the timing for signing of the Root Zone is not dependent on any other. However, since the Root Zone is at the top of the DNS hierarchy, it should be signed as soon as possible since this will facilitate verifying a chain of trust from the Root Zone Public Key[1]. Any DNS resolver on the Internet that configures the Root Zone Public Key as a Trust Anchor will be able to perform this verification. This document specifies various alternative methods, including software alternatives that can be used to sign the Root Zone.

1.1 Goals and Objectives

In order to achieve an operational DNSSEC signed Root Zone, changes need to be made to the existing process that is used for maintaining and changing the content of the Root Zone. This specification focuses exclusively on this aspect of achieving a signed Root Zone. Since the process for changing and maintaining the content of the Root Zone is outside the scope of this specification, this document only addresses aspects of the Root Zone content process that relate to DNSSEC. Additionally, this specification was developed with the intent of minimizing changes to the existing process. When a particular activity could be accomplished in different ways, minimizing changes to the existing processes was the dominant factor in selecting the specific method. This specification recommends the use of open source or implementation reviewable commercial software as much as is reasonable so that any interested party will be able to examine tools used in the Root Zone signing process. The opportunity to examine the software used in the process should significantly help build international support for the continuing Department of Commerce (DoC) role in the Root Zone management process.

1.2 Context and Background

DNS is a hierarchical, replicated and distributed database that maps between a human-memorable domain name and some information about that name, for instance an IP address. It forms one of the core infrastructure components that enable the Internet to be as useful as it currently is.

DNS in its native form is extremely insecure. Packets can be intercepted, clients can be betrayed by malicious or compromised servers and databases can be corrupted causing servers to give out incorrect responses to queries. Fallouts from these threats range from minor inconveniences for users to that of financial loss from downtime, embarrassment from having been attacked, to major attacks on user systems and applications and, in the worst-case, compromise of homeland or national security.

DNS Security is the result of the focused effort of the security community and DNS operations community to add security to the DNS protocol. These extensions provide origin authentication and data integrity by associating cryptographic signatures with the DNS information. Consumers of this information can check these signatures to gain assurance that the data was created by an authorized entity and that the data was not modified in any way from the time of creation by the authorized entity. Other security extensions include transaction authentication, which provides

[1] This is the public portion of the Root Key Signing Key, as described later in this document.

assurance that messages sent between the DNS servers or between DNS servers and clients are not modified in transit.

The rest of this document assumes a general understanding of DNS and a high-level understanding of DNS Security. For additional information on DNS Security, see Request for Comments (RFC) 4033[8], 4034[9], and 4035[10].

1.3 Document Roadmap

This document uses functional names for organizations involved in the Root Zone maintenance and change process, the Root Zone signing process and the Root Zone distribution process.

This document is organized as follows. Section 2 describes the current Root Zone update and maintenance process that is related to DNSSEC and provides a roadmap for signing the Root Zone. Section 3 provides some basic background for what it will take to sign the Root Zone. Section 4 discusses some of the threats to the signed Root Zone and threats associated with the root signing process. Sections 5 though 7 describe the architectural, technological, operational and organizational details, along with a small number of alternative options. Appendix A gives a list of the functional names and their meaning, as well as defining acronyms. Appendix B maps the functional names to the organizations that perform or are expected to perform the functions. Appendix C provides additional information related to the possibility of multiple Root Key Operator organizations.

2 Background

2.1 Current Process

The current process for modifying and publishing the Root Zone is very structured. This process involves a number of organizations with each one having a specific function in the overall process. A simplified diagram of this process is shown below in Figure 1. The organizations are named generically in this document. The organizations currently performing these functions are listed in Appendix B.

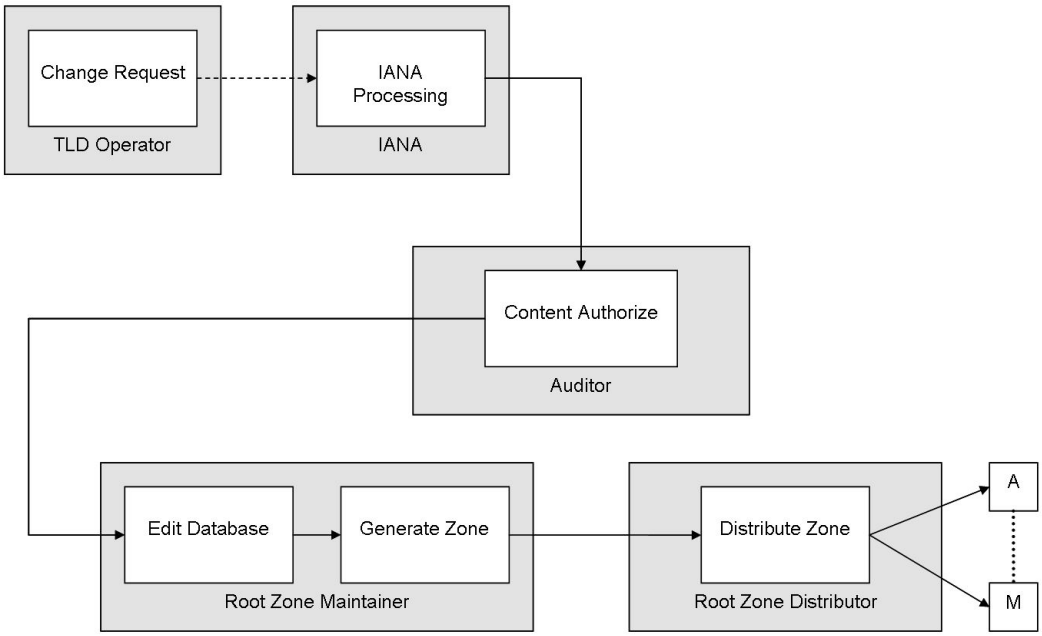

Figure 1: Current Process Flow

2.1.1 Steps

The steps in Figure 1 are grouped by the organizations that perform them. Each step is discussed below.

2.1.1.1 Change Request

At present, the primary requests for changes come in from Top Level Domain (TLD) operators. Occasionally, other requests are received from root server operators to change their lists of name servers. Re-delegation requests also arise occasionally from other sources. Additionally, changes in the operation of a name server providing look up service for one or more TLDs may require changes to the glue records. The processes for initiating such changes are under review by appropriate activities and are outside the scope of this specification. For purposes of this document, the variations in where change requests originate from are not important.

2.1.1.2 IANA Processing

Once IANA, also known as Internet Assigned Numbers Authority, receives a change request, the processing begins. This processing involves validating the requested changes and then forwarding the request via PGP-signed email to the Auditor for authorization.

2.1.1.3 Content Approve

The Auditor performs a check on the change request and then forwards the request by PGP-signed email to the Root Zone Maintainer (RZM) for completion.

2.1.1.4 Edit Database

The RZM takes the change request and makes the changes to the database that stores all of the data for the Root Zone.

2.1.1.5 Generate Zone

The RZM then generates a new Root Zone file from the data contained in the database and passes it to the Root Zone Distributor (RZD). The Root Zone generation process is repeated as per a well-defined schedule, even when there are no changes to the zone content. The Root Zone is regenerated in accordance with current policies.

2.1.1.6 Distribute Zone

The RZD loads the new Root Zone file into a Distribution Master Name Server and the 13 current root name server clusters (named A through M) are notified that the file has been updated via the DNS protocol. The root name servers then transfer the new Root Zone file from the Distribution Master name server.

2.2 Root-Signing Roadmap

Full operation of DNSSEC at the Root level requires several component capabilities. Both key signing and zone signing keys (KSK and ZSK) need to be generated. The public part of the KSK needs to be distributed to the community and used by resolvers everywhere. The software, hardware, and procedures within the IANA, RZM, RZD and the root server operators need to be modified to accommodate DNSSEC. To set up signed delegations for Top Level Domains (TLDs), the hashes of the keys of the TLDs have to be acquired in a trusted manner, incorporated into the signed Root Zone, and published in the Root Zone.

Reaching these capabilities fits into seven inter-related stages, as depicted in Figure 2.

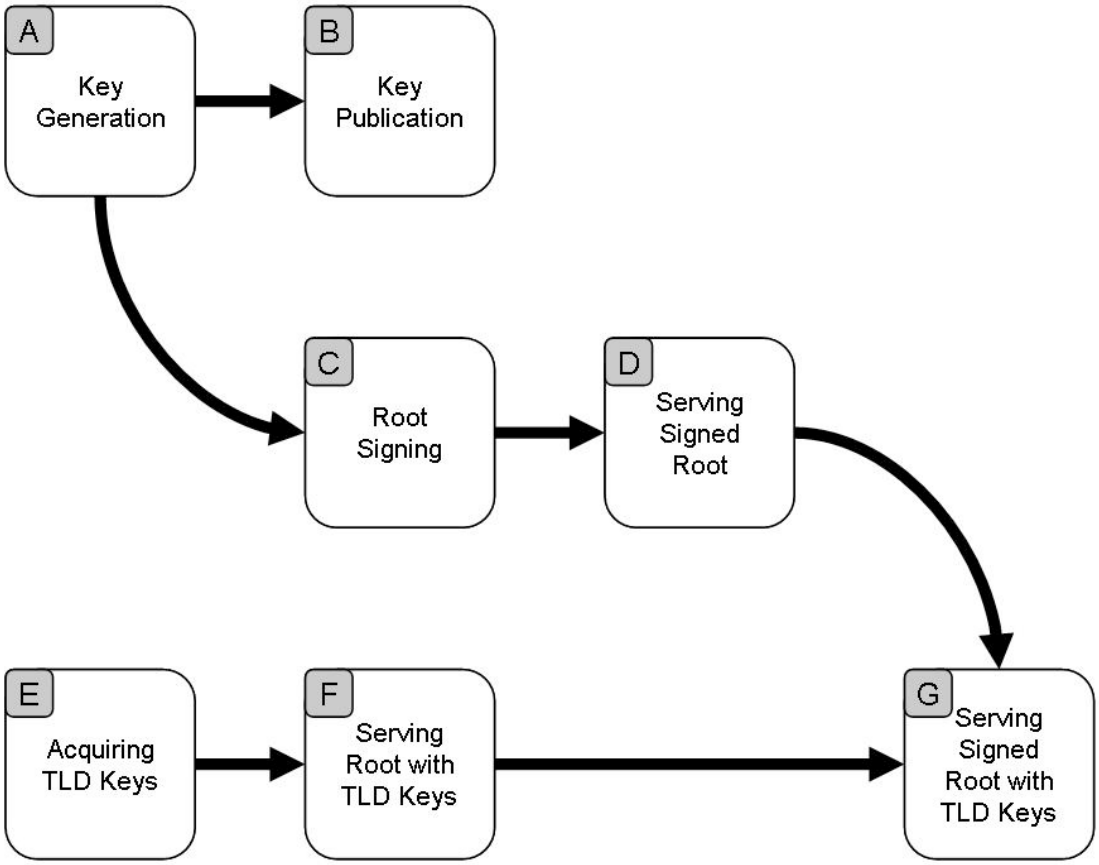

Figure 2: Roadmap for Signing the Root Zone

For most of these stages, there are technical or policy issues, software, and/or hardware to be created or acquired, operational procedures to be adopted, and testing done before complete operation is reached. The arrows show dependencies to reach full capability, but within each stage preparations can take place before the prior stage is complete.

Specific requirements for each of these stages are listed below.

A. Key Generation

This stage specifically refers to the generation of the Key Signing Key (KSK).

Issues: Organization control of the process, key length and lifetime, possible use of split key or other safety mechanisms, use of hardware versus software for generation, and storage and access requirements.

B. Key Distribution

The public portion of the KSK has to be distributed to the entire community, so that resolvers across the Internet can configure it as a Trust Anchor. This stage covers the distribution process, including replacement of the key (rollover) on both a regular and non-scheduled basis.

Issues: Automatic versus manual rollover, key distribution mechanism.

C. Root Signing

This is the process of signing the Root Zone assuming the root Key Signing Key (KSK) is available. Completion of this stage requires generation of the Zone Signing Key (ZSK), signing it using the KSK and having the hardware and software in place to use the ZSK to generate a signed zone. This stage involves addition to or modification of the processes and procedures in place at organizations involved in the Root Zone maintenance process.

D. Serving Signed Root

Twelve root server operators operate the thirteen root server clusters which total more than one hundred geographically dispersed root name servers. Each of these has to be capable and ready to properly answer queries that require DNSSEC signed answers.

Each of the root server operators has either completed or is in the process of upgrading its systems to be able to handle DNSSEC queries/answers. As of the date of this draft, about half are either ready or will be within six months. The other half are waiting for strong indication that DNSSEC is coming.

E. TLD Key Acquisition

This stage is acquisition of hashes of TLD keys from the TLD zones. This stage requires processes and procedures for interacting with the TLD operators. (There is some controversy whether this step is desirable. That is, does it make sense for the root servers to provide the keys of the TLDs if they are not signed by the root key? This stage is included here for completeness in the sense that it's logically possible for the IANA to acquire keys from the TLDs and for the root servers to be ready to answer DNSSEC queries but the root is not signed. If the root is signed, stage E will lead immediately to stage G.)

F. Serving Root with TLD Keys

The Root Zone can begin publishing TLD keys, even before the Root Zone itself is signed. This step refers to the scenario, where at least some of the TLDs are signed, but the Root is not signed, and the Root Zone publishes the Delegation Signer (DS) records for the TLD keys.

G. Serving Signed Root with TLD Keys

This is the natural culmination of the process when the entire Root Zone, along with the DS records for the TLD keys, is signed. When stages D and F are complete, this stage should be essentially automatic.

The remaining sections in this document lay out various architectural, technical, operational, and organizational options for achieving a signed Root Zone.

3 Root-Signing Basics

Since the Root Zone is at the top of the DNS hierarchy, it should be signed as soon as possible since this will facilitate verifying a chain of trust from the Root Zone Public Key[2]. Any DNS resolver on the Internet that configures the Root Zone Public Key as a Trust Anchor will be able to perform this verification.

3.1 Types of Root Keys

There are two sets of keys that will be used to sign the Root Zone. The first type of key is called the Key Signing Key and the second type of key is called the Zone Signing Key. A description of each of these key types follows. Each key is actually a public/private key-pair. The public portions of both types of keys are published in the Root Zone. This set of public keys is called the Root Keyset. The private portions of these keys are stored securely and are used for signing purposes.

3.1.1 Key Signing Key

The private portion of the Key Signing Key (KSK) is used to sign the Root Keyset published in the Root Zone. The KSK public key will be the "Root Zone Public Key" and will be published via various means and configured into security-aware DNS resolvers as a Trust Anchor. The public portion of the KSK will be included in the Root Keyset and published in the Root Zone.

3.1.2 Zone Signing Key

The private portion of the Zone Signing Key (ZSK) is used to sign all of the non-DNS-key data in the Root Zone. The public portion of this key should never be configured as a Trust Anchor by any DNS resolver. In keeping with the specifications for DNSSEC, the Key Signing Key, as a part of the Root Keyset, signs the Zone Signing Key. Public keys of future ZSKs may be published in the Root Keyset to assist in ZSK rollovers.

3.2 Key Life Stages

Each key (KSK or ZSK) has the following life stages:

1. Generation: The key is generated.
2. Publication: The public portion of the key is added to the Root Keyset and the Root Keyset is published. The public portion of the KSK is also published via non-DNS channels.
3. Use: The private portion of the key is used to sign data (the Root Keyset in case of the KSK and the Root Zone in case of ZSK).
4. Retirement: The private portion of the key is no longer used for signing data.
5. Removal: The public portion of the key is taken out of the Root Keyset.

Each of these stages needs to be managed properly by the Root Zone signing process. Multiple organizational entities may be involved in each of these stages, as described below in Section 5.

[2] This is the public portion of the Root Key Signing Key, as described later in this document.

4 Threats to the Signed Root

The Root Zone has a critical role in the proper functioning of the DNS services. For this reason the security of the Root Zone and the Root Zone signing process requires extra attention. The integrity and availability requirements of the Root Zone contents are extremely high. Because of this the Root Zone signing process also has stringent security requirements. The first step in determining these requirements starts with a thorough look at the threats to both the Root Zone and the Root Zone signing process.

The processes associated with obtaining a signed Root Zone are new. Because these processes are new, they are natural target for attack. Theses new processes can potentially introduce new vulnerabilities or new attack points. The introduction of DNSSEC adds new timing constraints to the architecture. These timing constraints require additional planning in order to allow for a smooth transitions.

Any discussion of security is normally focused around confidentiality, integrity and availability. Confidentiality deals with privacy and access control issues. Since the information being protected by the DNSSEC related processes, i.e., the content of the Root Zone, is public, confidentiality of the Root Zone is not an issue. Since existing processes deal with the appropriate protection of the content of the Root Zone, this essentially provides the required authorization controls for the content. Data integrity is one of the primary focuses of DNSSEC; therefore, the security issues that surround the integrity of the root data are top priority. Availability is a serious issue for any infrastructure service and, as such, is dealt with through the use of redundancy measures such as anycast deployment for name servers.

This document assumes that existing security practices, for the various the organizations participating in this process, are currently being followed. However, an independent Threat Analysis and Risk Assessment should be considered for the various participating organizations to provide a more in-depth assessment of operations.

4.1 Threats to the Signed Root

The following list and sub-lists enumerates threats to the Signed Root:

1. Adding/removing/changing keys process corruption.
2. Alternate Roots
    a. Adding RRs to signed RRset breaks validation
    b. Adding keys
        i. Works only if they are installed as TA in validators
        ii. May cause confusion in validators that have the real root TA
        iii. May be using different rollover procedures
            1. Which may break validators
            2. Root rollovers may break alternate root validators
    c. May strip official key/RRSIGs and resign using different keys
        i. Cannot be stopped, but will only be validated by clients that have the keys
3. Local redirection of root
    a. Done by some local networks (hotels for example) that intercept DNS queries and redirect it to a local version of root or gTLD's
    b. Moderate risk, but not as malicious attack
    c. Could cause validators to fail
        i. Or may work if local server is not DNSSEC aware (just have no signatures in responses)
4. Compromise of the signing algorithm.
5. Private Key compromise
    a. Private key destruction
    b. Private key modification

6. Public key publishing mechanism compromise
    a. Public key modified
    b. Public key not available
7. Potential Reflector Target
    a. Increased amplification factor due to location in DNS hierarchy
    b. Ability to generate large volumes of traffic

4.2 Threats to the Root Signing Process

The following list and sub-lists enumerates threats to the Root Signing Process:

1. False reports of compromised key.
2. Procedural abuse causing unnecessary work or distraction by RKO, auditor and RZM. Since the process is new this procedural abuse could be a type of denial or service behavior, especially since many of the actions taken are time based. Details are not yet fully known nor has this behavior been exhaustively tested.
    a. Thrash for client validators.
3. Weakness found in communication links between entities.
4. Disruption of communication links between entities.
    a. Slow down operations.
        i. Must disrupt communication for 30 days for – timers rollover scheme to fail.
    b. May be used in conjunction with some other attack.
5. Insider attacks/User error
    a. IANA-like process inserting/altering change request from TLD operators.
    b. Content Auditor altering data.
    c. RZM altering change request or making input error.

5 Architectural Options

This section describes the overall architecture of the Root Zone signing process. In order to minimize changes to the current Root Zone creation process, this specification primarily adds steps to the existing process and makes small changes to existing responsibilities and workflow. The additional steps have been kept as modular as possible so that future extensions will require minimal changes.

A significant addition to the existing architecture in this specification is the function of the "Root Key Operator" (RKO). The RKO will be responsible for the generation and use of the Root Zone Key Signing Key (KSK), which is the top-level key for the entire DNS hierarchy. This new function could, in principle, be assigned to a variety of organizations.

Although it is theoretically possible to have multiple RKOs, the operation is much more complex and not recommended. Appendix C provides additional detail related to the possibility of multiple RKO organizations. At this point, further research and prototyping is required to determine whether or not multiple RKOs would be operationally feasible and whether or not potential benefits would be worth the additional complexities.

While the KSK is the top-level key for the DNS hierarchy, the Root Zone Signing Key (ZSK) performs the day-to-day signing of the Root Zone. There are three possible architectural options based on where the generation and use of the ZSK takes place. They are:

1. The Root Zone Maintainer (RZM) generates and uses the ZSK to sign the Root Zone. In this case, the RZM will need to securely transfer the public part of the ZSK to the RKO so that the RKO can sign the entire Root Keyset.
2. The RKO generates the ZSK and transfers it securely to the RZM, which then uses it to sign the Root Zone. This will involve secure transfer of the private part of the ZSK from the RKO to the RZM.
3. The RKO generates and uses the ZSK to sign the Root Zone. Since the Root Zone file is currently generated from a database held by the RZM, this option will require secure transfer of the Root Zone between the RZM and the RKO.

These three options are described in detail below.

5.1 Option 1: RZM creates ZSK and signs Root Zone

In this option, the Root Zone Maintainer (RZM) generates and uses the ZSK to sign the Root Zone. The advantage of this scheme is that it keeps the key generation and use functions together, a desirable security practice.

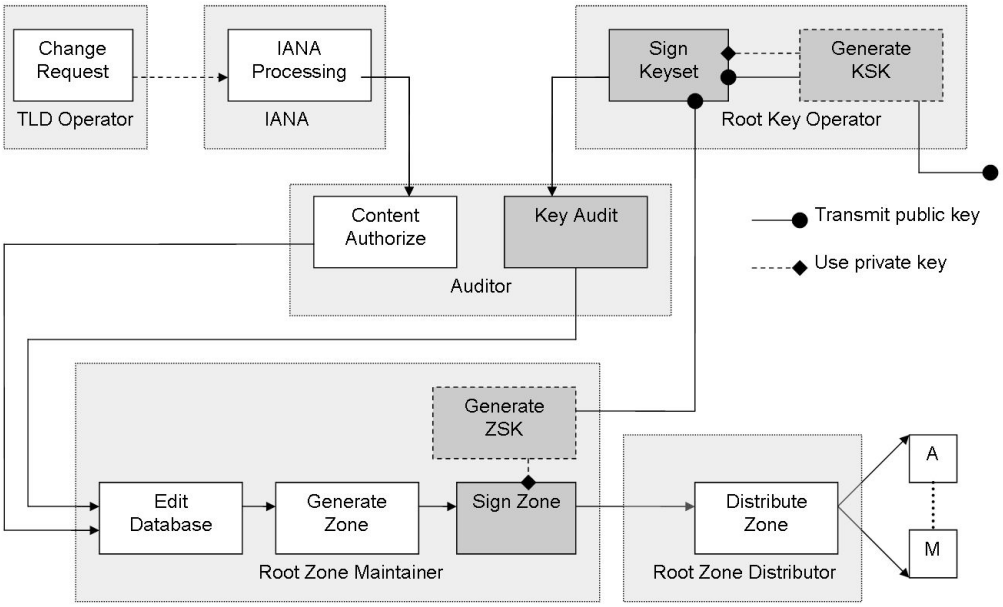

Figure 3: Proposed Process Flow – Option 1

The RZM will be entirely responsible for the ZSK in accordance with a contracted set of rules and procedures. It will need to store the private portion of the ZSK in a secure place, use it to sign the Root Zone, and provide for scheduled and non-scheduled procedures for ZSK rollover. Whenever the ZSK changes, the RZM will need to transfer the **public** portion of the ZSK to the RKO so that the RKO can sign the entire Root Keyset. This transfer needs to be over a trusted channel that provides authentication, data integrity, non-repudiation, and ideally, delivery assurance.

This revised process adds five additional functions to the Root Zone maintenance process: Generate KSK, Generate ZSK, Sign Keyset, Key Audit and Sign Zone. These additional functions are shown in grey-colored boxes in Figure 3, and are described in detail in Section 5.4.

5.2 Option 2: RKO creates ZSK and RZM signs Root Zone

In this option, the RKO generates the KSK and ZSK. The RKO generates the Root Zone Keyset and transfers it and the ZSK securely to the RZM, which then uses the ZSK to sign the Root Zone. This scheme keeps all the root-key generation functions at one place as the RKO generates both the KSK and the ZSK. The disadvantage of this scheme is that it requires a secure transfer (including confidentiality encryption) of the private portion of the ZSK from one organization to another. It will also require secure storage of the private key of the ZSK at two geographically separated places – at the RKO and at the RZM. This adds complexity to the root-signing process and increases the probability of a ZSK key compromise.

Most of the responsibilities and information flow in this scheme are similar to the previous one. The details of the individual functions are similar to Option 1.

As the RKO generates the ZSK, it will be able to generate the entire Root Keyset for the Root Zone on its own. The RKO will need to transfer the **private** portion of the ZSK to the RZM in a secure manner. Security here means confidentiality (encryption), authentication, data integrity, non-repudiation, and delivery assurance. This transfer may or may not pass through the Key Audit function. The RZM will still need to maintain the ZSK: (a) accept the **private** portion of the ZSK from the RKO to sign the Root Zone, and (b) store the **private** portion of the ZSK securely. The RZM will need to communicate with the RKO in the event of any situation of possible ZSK compromise, so that the RKO can initiate a non-scheduled ZSK rollover.

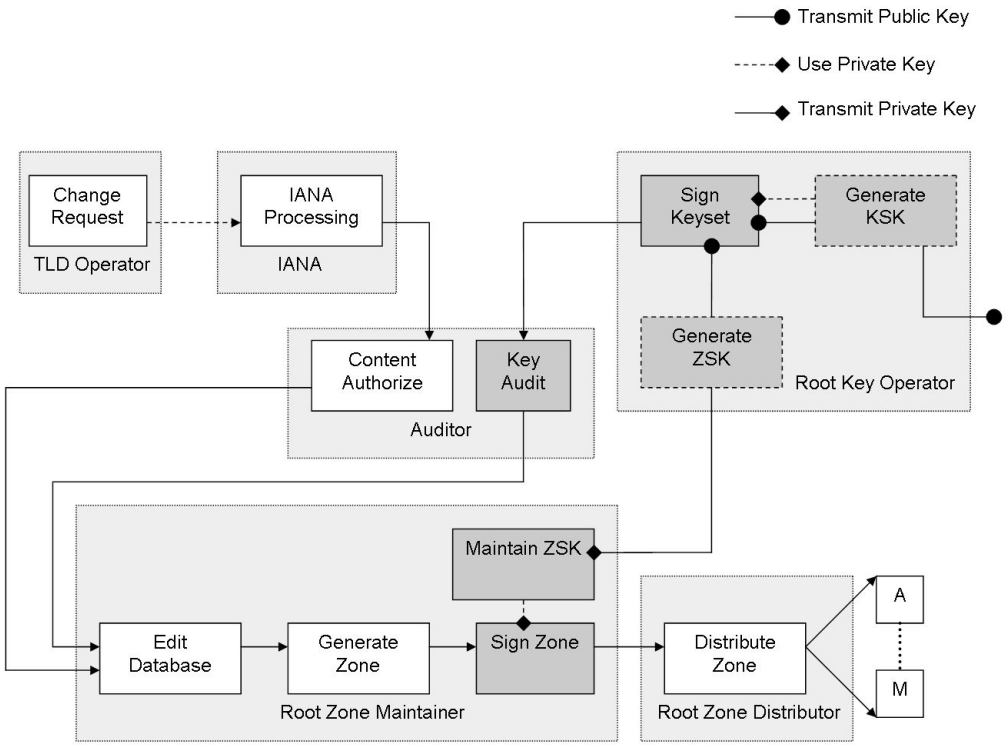

Figure 4: Proposed Process Flow – Option 2

This revised process adds six additional functions to the Root Zone maintenance process: Generate KSK, Generate ZSK, Sign Keyset, Key Audit, Maintain ZSK and Sign Zone. These additional functions are shown in grey-colored boxes in Figure 4, and are described in detail in Section 5.4.

5.3 Option 3: RKO creates ZSK and signs Root Zone

In this option, the RKO generates the KSK, the ZSK and uses the ZSK to sign the Root Zone. The advantage of this option is that it will keep the generation and use of the private portions of the KSK as well as the ZSK with a single organization, a desirable security practice. The disadvantage of this option is that it will require frequent (on the order of multiple times per day) secure zone transfers between the RZM and RKO.

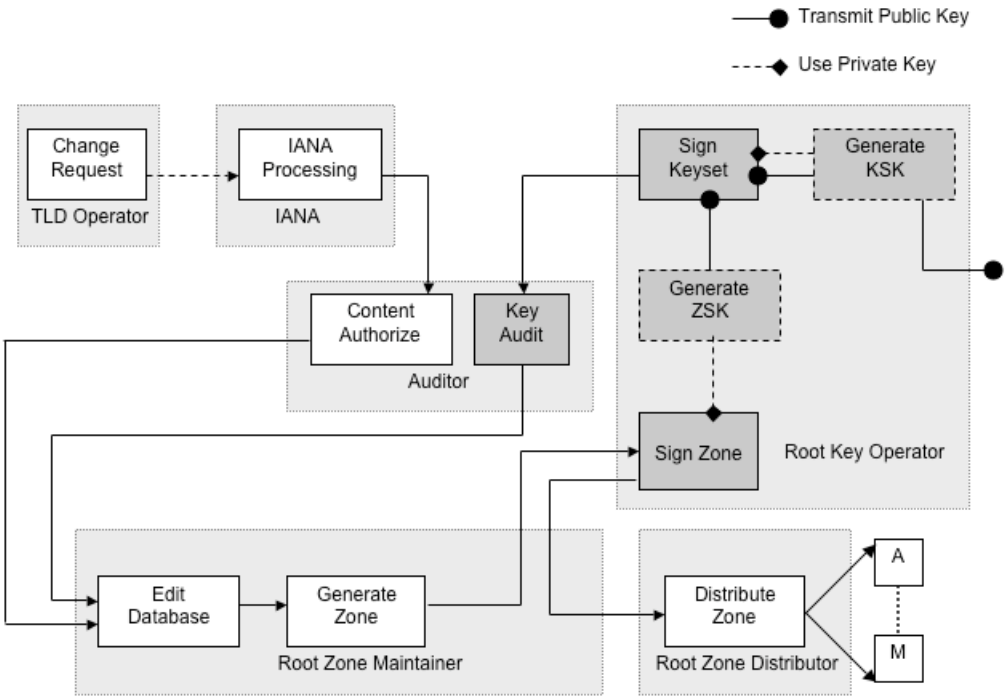

Figure 5: Proposed Process Flow – Option 3

This revised process adds five additional functions to the Root Zone maintenance process: Generate KSK, Generate ZSK, Sign Keyset, Key Audit and Sign Zone. These additional functions are shown in grey-colored boxes in Figure 5, and are described in detail in Section 5.4.

5.4 New Functions

The above options for the root-signing process add six steps to the existing process. The first step "Generate KSK" is performed when the root's Key Signing Key needs to be changed. The second step "Generate ZSK" is performed when the root's Zone Signing Key needs to be changed. The third step, "Sign Keyset" is performed periodically as well as whenever one of the keys associated with the Root Zone changes. However, changing keys is not coupled to the normal Root Zone modification and zone file generation process. The fourth step "Key Audit" occurs whenever the RKO sends a signed Root Keyset template to the Auditor. The fifth additional step, "Sign Zone", is coupled to the existing Root Zone file generation process and is performed periodically as well as every time a change is made to the content of the Root Zone. These steps are discussed below.

Option 2 adds another step called "Maintain ZSK", which will be carried out by the RZM. This will involve storing the private portion of the ZSK securely, and initiating non-scheduled rollover

in case of a ZSK compromise. One security best practice that should be followed is that any keys generated should not be exported from the cryptographic modules where they are generated. Option 2 does not conform to this best practice. The motivation, however, for Option 2 is that key generation for both the KSK and ZSK, possibly the most sensitive part of the process, is under the control of a single, presumable highly-trusted, organization.

Setting up secure delegations for the TLDs from the root, as described in the roadmap (Section 2.2), requires various functions in the Root Zone maintenance process to be able to accept and process DS records for TLD keys. This will be part of the normal Root Zone data update process, and hence will not be described here.

5.4.1 Generate KSK

The RKO is responsible for generating and maintaining the root KSK. It stores the private portion of the KSK securely, and publishes the public portion of the new KSK via non-DNS channels. The generation of a new KSK may trigger the Sign Keyset step, if it is part of a scheduled KSK rollover, in which case the old (current) KSK will be used to sign the Root Keyset. The RKO is responsible for changing the KSK periodically according to a well-defined schedule, as well as in response to unexpected situations requiring a non-scheduled change.

The new KSK can be used to sign the Root Keyset only after a time lag, to enable security-aware DNS resolvers across the Internet sufficient time to acquire the new KSK key and have it configured as a Trust Anchor. If it is a new (first) KSK or a non-scheduled rollover, the public portion of the KSK needs to be published first via one or more non-DNS channels. For a scheduled rollover, in addition to the non-DNS channel, the public portion of the new KSK should be published in the Root Keyset for some time, before it is used for signing the Root Keyset.

KSK generation should be performed on a physically protected machine that should be disconnected from the Internet. Within this general prescription various implementations are reasonable, ranging from software key generation to specialized hardware devices. Multiple additional copies of the key must be created and stored securely in other separate locations.

The Operational Options section below discusses various aspects of the KSK, such as the algorithm and length of the KSK, schedule for changing the KSK, and a list of unexpected situations when the KSK needs to change.

5.4.2 Generate ZSK

The RZM (option 1) or the RKO (options 2 and 3) generates a new ZSK periodically according to a well-defined schedule, as well as in response to unexpected situations. The private portion of the ZSK is stored securely, and is used to sign the Root Zone. In option 1, the public portion of the ZSK needs to be transferred from the RZM to the RKO over a secure channel that is trusted to provide authentication, data integrity, non-repudiation, and assurance of data delivery. In option 2, the private portion of the ZSK needs to be transferred securely from the RKO to the RZM over a trusted channel that provides confidentiality encryption, authentication, data integrity, non-repudiation, and delivery-assurance.

ZSK generation should be performed on a physically protected and isolated machine, i.e., one that is not connected to the Internet. Key generation can be done using a tool that correctly creates the public/private key pair needed by DNSSEC and the DNSKEY Resource Record (RR). Additional copies of the ZSK should be securely stored in other separate locations to guard against hardware and/or software failures.

Once the ZSK is generated, its public portion will be included in the Root Keyset and will be signed by the RKO. The signed Root Keyset will be published as a part of the Root Zone. At any given time, the Root Keyset will contain two ZSKs – one current and one future. Publishing the future ZSK ahead of time will facilitate the scheduled rollover of the ZSK.

A discussion about various aspects of the ZSK, such as the algorithm and length of the ZSK, schedule for changing the ZSK, and a list of unexpected situations when the ZSK needs to change, can be found in the Operational Options section below.

5.4.3 Sign Keyset

Whenever the ZSK or the KSK changes as per a scheduled rollover, the Root Keyset will need to be updated, re-signed, and the Root Zone will subsequently need to be republished. The Root Keyset will also need to be re-signed before the current signature expires. The following sub-steps comprise this step:

1. The RKO builds the Root Keyset from the current ZSK public keyset and the KSK public key.
2. The RKO transfers the Root Keyset to the machine used for signing via a trusted and secure mechanism.
3. The Root Keyset is signed using the private portion of the KSK. If this 'Sign Keyset' step was triggered because of the generation of a new KSK as a part of a scheduled KSK rollover, the old KSK will be used to sign the Root Keyset.
4. The signed Root Keyset template (which includes the Root Keyset and the KSK-signature on the Root Keyset) is transferred off the key-signing machine via a trusted and secure mechanism.
5. The signed Root Keyset Template is transferred to the Key Audit function via a trusted channel that provides authentication, data integrity, non-repudiation, and assurance of delivery.

The Root Keyset also needs to be re-signed periodically as per a well-defined schedule. This re-signing takes place before the current KSK signature expires. The periodicity of this process will mean that the Key Audit function and the RZM should be able to receive periodic updates of the signed Root Keyset template. The Operational Options section below discusses the possible values for signature lifetime and re-signing frequency.

5.4.4 Key Audit

The Key Audit function will be responsible for auditing signed Root Keyset templates generated by the RKO. The sub-steps for the Key Audit function are:

1. Accept a signed Root Keyset template from the RKO over a trusted channel that provides authentication, data integrity, non-repudiation and delivery assurance.
2. If the KSK or ZSK has changed, verify that it satisfies the operational parameters regarding key-length, algorithm etc.
3. Verify that the signature lifetime follows the operational parameters, and that the signature can be verified using the current KSK. The signed Root Keyset template will include:
   - Root Keyset which includes the public portions of the KSK and ZSK(s)
   - Signature on the Root Keyset using the KSK
4. Send the signed Root Keyset template to RZM over a trusted channel that provides authentication, data integrity, non-repudiation, and delivery assurance.

The Key Audit function will need to be able to accept the signed Root Keyset template (a set of DNSKEY record templates and an RRSIG record template). Additional responsibilities for the Key Audit function may be included in future versions of this draft. The transparency of the Key Audit function will be a desirable part of this process to ensure trust in the KSK.

5.4.5 Sign Zone

Each time a change is made to the content of the Root Zone, it needs to be re-signed before it is published on the Root Name Servers. The Root Zone also needs to be re-signed before the current ZSK signature expires. The Sign Zone step is thus both change driven and schedule driven. The following sub-steps comprise this step:

1. The RZM transfers the Root Zone file generated from the database to the machine used for Root Zone signing via a trusted and secure mechanism. This Root Zone file will contain DS records for TLDs and the signed Root Keyset in addition to the existing records. In option 3,

this will involve Root Zone transfers between the RZM and the RKO over a trusted channel that provides authentication, data integrity, non-repudiation, and assurance of delivery.
2. The Root Zone is signed using a tool that correctly generates the RRSIG and NSEC RRs. In options 1 and 2, the signing is done by the RZM. In option 3, the signing is done by the RKO.
3. The signed Root Zone file is transferred to the RZD for distribution to the Root Name Servers via a trusted channel that provides authentication, data integrity, non-repudiation, and assurance of delivery.

Signing of the Root Zone is a periodic process, determined by the operational parameters. It takes place before the current ZSK signature expires. The Operational Options section below discusses the possible values for signature lifetime and re-signing frequency.

5.5 New Events

The following are new events that will trigger information flow in the revised process:

1. A new KSK is introduced or a non-scheduled KSK rollover takes place
2. A scheduled KSK rollover takes place
3. A new ZSK is introduced or a non-scheduled ZSK rollover takes place
4. A scheduled ZSK rollover takes place
5. The Root Keyset is re-signed
6. The Root Zone is re-signed
7. A TLD provides a new KSK, or performs its KSK rollover

6 Technological Options

This section lists options for additional hardware and software pieces that will be needed to sign the Root Zone. It is sub-divided according to the organizations that perform various functions.

To set up signed delegations from the Root Zone, the signed Root Zone will also need to include the Delegation Signer (DS) records for signed TLDs. To make this possible, IANA, the Content Authorizer, and the RZM will need to be able to handle DS records for the TLDs. Since DS records are similar to other content of the Root Zone, this will require minimal changes in the organizations involved. Similarly, the RZD and Root Name Servers will need to support DNSSEC-specific Resource Records. The requirements for these changes are beyond the scope of this document.

6.1 Root Key Operator

The RKO is responsible for generating the KSK, signing the Root Keyset and communicating the signed Root Keyset to the Key Auditor. In architectural options 2 and 3, the RKO is also responsible for generating the ZSK.

Requirements:

- Since the integrity of the KSK is extremely important, all cryptographic hardware and software used at the RKO must be FIPS 140-2 Level 3 compliant [25].
- A software or hardware tool for generating keys.
- A software or hardware solution for storing and retrieving the private keys securely.
- A software tool for generating a DNSKEY Resource Record and for combining the DNSKEY Resource Records into a Root Keyset.
- A software or hardware solution for signing the Root Keyset.
- Trusted and secure communication mechanisms for transferring information to other organizations.

Based on these requirements, various solutions are possible. Various options to satisfy each of these requirements are given below. However, any other comparable solution that satisfies the above requirements can be considered.

Key Generation

- OpenSSL [13] for generating keys.
- RSA BSAFE [23] cryptographic library from RSA Security for generating keys.
- Microsoft Cryptography API
- Perl Security and Encryption Modules

Key Storage and Retrieval

- OpenSC [14], OpenCT [15], smart cards, smart card reader for storing and retrieving private keys.
- nShield [22] hardware security module from nCipher for storing and retrieving keys securely.

Root Keyset Generation and Signing

- Tools from BIND [17] (9.3.1 or higher version) to create a DNSKEY RR, and assemble the DNSKEY RRs of all Root Keys (KSK and ZSK) into a keyset. Signing utility from BIND [17] (9.3.1 or higher version) that uses OpenSSL commands to sign the keyset and generate a signed Root Keyset Template.

- Tools from ANS [18] (2.5.0 or higher version) to create a DNSKEY RR, and assemble the DNSKEY RRs of all Root Keys (KSK and ZSK) into a keyset. Signing utility from ANS [18] (2.5.0 or higher version) for signing the keyset and generating a signed Root Keyset Template.

Communication between the RKO and the Key Auditor needs to be via a trusted channel that provides authentication, data integrity, non-repudiation, and delivery assurance. The communication between the RKO and the RZM in architectural option 2 would additionally require confidentiality encryption to transfer the private portion of the ZSK.

6.2 Key Approver

The Key Auditor accepts the signed Root Keyset from the RKO and forwards it to the RZM.

Requirements:

- Tools to verify the KSK signature over the Root Keyset.
- Tools to verify various properties of the keys such as key-length and algorithm.
- Tools to verify various properties of the signature, such as the signature lifetime.
- Communication software to verify that the signed Root Keyset came from the RKO and to securely send a signed Root Key Template to the RZM.

Options for Signature Verification

- BIND [17] (9.3.1 or higher version)
- ANS [18] (2.5.0 or higher version)
- Perl Module NET::DNS::SEC

It is recommended that different types of DNS software be used for this verification to ensure interoperability of the signed Root Keyset in the heterogeneous Internet environment.

6.3 Root Zone Maintainer

In architectural option 2, the RZM is responsible for accepting the private portion of the ZSK from the RKO. In architectural options 1 and 2, the RZM is responsible for signing the Root Zone. In architectural option 3, the RZM does not sign the Root Zone, hence does not need the hardware and software specified here, except for the secure communication software.

Requirements:

- A software or hardware tool for generating keys, if using architectural option 1.
- A software or hardware solution for storing and retrieving the private keys securely.
- A software or hardware solution for signing the Root Zone.
- A software tool for verifying the correctness of the signed Root Zone before it is published.
- Secure communication mechanisms for exchanging information with other organizations.
- Whichever tools are used for key generation and zone signing must use an approved cryptographic library.

ZSK Generation

- OpenSSL [13] for ZSK generation, if using option 1.
- RSA BSAFE [23] cryptographic library from RSA Security for generating keys, if using architectural option 1.

Key Storage and Retrieval

- OpenSC [14], OpenCT [15], smart card reader and smart cards for storing and retrieving the private portion of the ZSK.
- nShield [22] hardware security module from nCipher for storing and retrieving keys securely.

Signing the Root Zone

- The `dnssec-signzone` tool from BIND [17] (9.3.1 or higher version), and the `zonesigner` script from DNSSEC-Tools [20] for signing the Root Zone (BIND uses OpenSSL's cryptographic library)
- ANS [18] (2.5.0 or higher version), or any commercial software that correctly creates a signed zone file, for signing the Root Zone.

Signed Zone Verification

- `Donuts` (from DNSSEC-Tools [20]) and/or Secure Zone Integrity Checker [21] (from NIST) for verifying the correctness of the signed zone file, before it gets sent to the RZD.

The RZM must also support secure communication mechanisms for accepting signed Root Keyset from the Key Auditor and for accepting the encrypted signed private portion of the ZSK from the RKO, if using architectural option 2.

6.4 Communication Options

The various organizations involved in maintaining the Root Zone and signing the Root all need to communicate. These communications need to be secure and authenticated.

Requirements:

- The communication of various messages across organizational boundaries will require a trusted channel that provides authentication, data integrity, non-repudiation, and delivery-assurance.
- In architectural option 2, the channel between RKO and RZM used for transferring the private portion of the ZSK will require confidentiality encryption, in addition to these features.
- The channel used for communication must be reliable, and provide sufficient redundancy and fault tolerance.
- The channel must ensure connectivity and have sufficient capacity to carry out the information exchanges properly.

Option 1: Over the network solution using PGP

- PGP [19] signed email.
- In architectural option 2, PGP encrypted and signed email to send the private portion of the ZSK from RKO to the RZM. This email should also contain an indication of when to start using the new ZSK for signing the Root Zone.

Option 2: Over the network using Shinkuro

- Shinkuro secure file transfer [33] from Shinkuro, Inc. This provides confidential, reliable acknowledged delivery of files between parties operating behind firewalls and integrates cleanly with other processes.
- This method is presently being used in the current prototype effort.

Option 3: Over the network solution using SSH

- SSH Tectia [24] secure file transfer solution from SSH Communications Security Corporation.

Option 3: Hand-delivery

- Hand-delivery can be an option, especially for transferring the private key from the RKO to the RZM. In this case, a copy of the smart card or other hardware media will be transferred from the RKO to the RZM in a secure and timely fashion.

7 Operational Options

There are various options for operational decisions that need to be made regarding signing the Root Zone. This section discusses those options.

7.1 KSK Publication

The public portion of the KSK needs to be published via multiple channels so that DNS resolvers across the whole Internet can read it and configure it as a Trust Anchor for verifying other DNS records. This publication of the KSK has to be via non-DNS channels. Examples include publishing it in newspapers, via a secure website, or signed copies by various well-known entities including Certificate Authorities.

7.2 Signature Algorithm

The signature algorithm must be a standard algorithm recommended for DNSSEC, so that security-aware DNS resolvers throughout the Internet can verify the signature. As an example, signature validation cost for resolvers is important because a very large number of resolvers Internet-wide will be performing these signature validations. Guidance on this topic is appropriate for a separate document.

7.3 Key Parameters

The key must be long enough to survive concerted attack even as technology improves. The size of the keys used will depend on a number of factors, including: which year it is, the time between key publication and removal, and the cost of signature validation in resolvers. As an example, signature validation cost for resolvers is important because a very large number of resolvers Internet-wide will be performing these signature validations. Guidance on this topic is appropriate for a separate document.

7.4 Key Rollovers

KSK Rollover

KSK rollover will occur on a periodic basis according to a well-defined schedule. When the KSK is rolled, the new public key will be included for signing as part of the Root Keyset. There must be a substantial time lag between introducing a new KSK and using it to sign the Root Keyset.

For the initial deployment, it is recommended that the KSK rollover process be carried out moderately frequently to test the process. “Moderately frequently” probably means every four to six months. When the process is stable, regular KSK rollovers should occur often enough to keep the key refreshed, probably every two years.

A process to automate trust anchor rollover is presently underdevelopment. If and when this process is complete the options presented will be updated to utilize the automated processes.

ZSK Rollover

ZSK rollover will occur on a regular basis according to a well-defined schedule. When the ZSK is rolled, the new ZSK public key will be included in the Root Keyset.

For the initial deployment, it is recommended that the ZSK rollover process be carried out once every month. When the process is stable, regular ZSK rollovers should occur often enough to keep the key refreshed, probably once every four to six months. There has to be a time lag greater than two times the TTL for the Root Zone DNSKEY set before a new published ZSK can be used for signing from the time it the copy of the root zone it appears in is distributed.

7.5 Signature Lifetime and Re-signing Frequency

A recommended frequency for re-signing the Root Keyset is once a week (7 days), with the validity period of each signature being 3 weeks (21 days).

An alternative to re-signing frequently is for the RKO to pre-generate signatures for the Root Keyset up to one year in advance, each signature beginning at the start of a week. The RKO can then send a batch of signed Root Keyset templates to the Key Audit function, which will authorize and forward it to the RZM. The RZM will then use one signed Root Keyset every week. The advantage of this scheme is that the RKO and Key Audit functions will have to communicate only infrequently (once a year, for example, or when ZSKs or KSK change). The disadvantage of this scheme is that the RZM will have to securely store these signatures and use the appropriate one each week. This might pose a security risk. Also, if there is a change in the ZSK or KSK, all the signed Root Keyset templates stored with the RZM will be invalid. Hence, the pre-signing scheme is not recommended.

As the Root Zone's SOA serial number is incremented twice a day, a reasonable frequency of re-signing the Root Zone is twice a day coinciding with the SOA serial number increment, with the validity period of each signature being 3 days.

7.6 Non-Scheduled Operations

The Root KSK is the top-level key of the DNS hierarchy and will be configured as a trust anchor in security aware resolvers across the Internet; hence every precaution must be taken so that unscheduled, forced KSK rollovers are never required. Even though Root ZSKs are not configured in resolvers, it is important that those rollovers also be as smooth as possible. Even with the greatest care there are multiple reasons why unscheduled rollovers may take place, examples include:

- A new signing algorithm is introduced.
- The contractor with access to private portions of Root Zone KSKs or ZSKs is changed.
- A weakness is suspected and/or found in the algorithms used.
- A key might have been compromised.
- The number of available spare Root Keys falls below a threshold. This may happen if there are hardware failures as well as if unpredictable events destroy a copy.
- An active attack is underway to break the Root Key and has a higher than acceptable chance of succeeding before the key is scheduled for retirement.

It is important that the handling of these events is timely in order to minimize interruptions in providing the secured DNS service. The overall root key and zone signing process has a number of delays built into it which cannot easily be bypassed, thus, any change will require some lead time. A change in the ZSK subset can be done relatively rapidly as it is only impacted by how long a new ZSK subset propagates through the root key signing system as well as the Root Zone signing process. A change in the KSK on the other hand takes a longer time as the new KSK has to be configured into resolvers all over with a world which can only take place after the operators of the resolvers have been convinced that the new KSK is valid

A timeline for these events needs to be created and processes ought to be put in place where the overall flow through the system can be accelerated under special circumstances for changes in the ZSK subset. For rapid deployment of a new KSK, a special publication plan must be ready along with a timeline of when each event will take place. Both of these types of nonscheduled events cannot be currently designed since they will be impacted by the organizational and contractual framework for the operations.

7.7 Operational and Physical Security

The private portions of the KSK and ZSK should be stored securely to prevent a compromise of these keys. Generation of a new KSK or ZSK should also follow appropriate requirements so that the keys are not compromised. For example, at least 3 out of a set of 5 people must sign off on a new KSK or ZSK. The private portions of the keys should be stored at multiple locations and on multiple media so that a given key is available even if one copy is destroyed.

These operational parameters should be transparent and well published in order to ensure the trust in the root keys.

8 Organizational Options

This section offers four options for the organizational structure of the Root Key Organization.

1. New unit within an existing governmental agency: The RKO is created as a self-sufficient unit within an existing federal agency. All functions — technical, policy, legal, and otherwise — pertaining to Root Zone signing are contained within the staffing structure of this unit and report to the head of the unit.
2. New unit within contractor (under contract to an existing governmental agency): The RKO is created as a self-sufficient unit within an existing non-government organization or as a new non-government organization. All functions — technical, policy, legal, and otherwise — pertaining to Root Zone signing are contained within the staffing structure of this unit and report to the head of the unit.
3. Existing governmental unit: The RKO functions are assigned to an existing governmental agency that has the capabilities to carry out significant portions of the mission, including an operations staff that functions 7 days per week, 24 hours per day, a secure facility, legal and communications staffs, and administrative support functions. Under this option, the unit chief may be able to assign some of the functions to existing elements within the agency. This option requires fewer new hires but may have more complex management challenges.
4. Existing unit within contractor (under contract to a governmental unit): The RKO functions are assigned to an existing non-government organization. Such an organization must have the capabilities to carry out significant portions of the mission, including an operations staff that functions 7 days per week, 24 hours per day, a secure facility, legal and communications staffs, and administrative support functions. Under this option, the existing staff of the contractor may be assigned some of the functions pertaining to root signing. As with option 3, this option requires fewer new hires but may have complex management challenges.

Most of the following describes the functions irrespective of these four options. The implications and resource estimates highlight significant differences between the new unit (1 and 2) and existing unit (3 and 4) options.

8.1 RKO Functions

The RKO's functions may be understood as: routine operations functions, supervisory and management functions, technology evolution, communications, policy/legal, and finance. Each of these functions is described in the following sections. The embodiment of these functions in an organizational structure and the resources required to support these functions are described Sections 8.2 and 8.3.

8.1.1 Daily/Routine Operations

Operationally, the RKO maintains equipment and processes to accomplish the following:

- Generate the public-private key pair for the root.
- Use the public portion relatively infrequently to create the root keyset for the key signing key and the zone signing keys.
- Store and protect the private portion of the key (KSK) in an appropriate manner.
- Publish the public portion of the key pair through multiple channels so that it can function appropriately in verification of signatures in resolvers.
- Use the private portion to sign the root keyset periodically and whenever any Root Zone KSK or ZSK changes.

If the organization of the proposed entity is structured to include generation and/or use of the ZSK (as well as the KSK); then appropriate changes to operations will be required.

These functions require a certain amount of hardware and software, an appropriate operational location to protect the equipment, adequate redundancy to protect against potential disasters and an operational staff capable and available to carry out this function. These resource requirements are detailed below (see Section 8.2).

8.1.2 Supervisory/Management Functions

In addition to the daily operations, there are a series of related support functions that are also necessary:

- Regularly scheduled key rollover.
- Non-scheduled key rollover.
- Post key rollover audit and review.
- Reporting.

Each of these support functions is described in the following paragraphs.

8.1.2.1 Routine Key Rollover Management

From time to time, it will be necessary to change the public-private key pair for the Root Zone. Good practice requires changing it on a regular basis, albeit not very often. This regularly scheduled event will be known in advance to the community but nonetheless will require additional oversight and attention, particularly the first few times to iron out any difficulties and build confidence. It will also be important to assess the primary impact of a key change for the community at large and on the resolvers that use the public key. The impact on the Root Zone operation is likely to be fairly modest but still must be addressed.

8.1.2.2 Non-Scheduled Key Rollover Management

Non-scheduled key rollovers pose several additional problems. First, the execution will be more stressful simply because it is not scheduled. Hence, additional attention will be needed to inform the community and perhaps to invoke procedures which are different from a scheduled key rollover. Second, the decision to actually initiate a non-scheduled Root Zone key rollover requires information, judgment and authority.

On the one hand, when a key rollover is necessary, it must be carried out without undue delay. On the other hand, unnecessary key rollovers impose a large cost on the community and reduce the credibility of the entire system. In the extreme, a rapid sequence of unnecessary non-scheduled key rollovers is an effective way to undermine the system. That is, it would be tantamount to a denial of service attack. Therefore, the decision to undertake a non-scheduled key rollover requires adequate information about the threat to the existing key and the ability to evaluate that information. The person making this decision must have sufficient authority to make the decision promptly. The information flow and expertise must be sufficient to provide the capability to make an informed decision and the person in this role must possess requisite authority to implement that decision and to defend it on technical and legal grounds.

Providing the right level of information to the decision maker requires input from the operational and intelligence communities that can raise the appropriate alarms regarding the safety of the current root key as well as help assessing any threats and vulnerabilities. The decision-maker also needs adequate resources within the organization to participate in these discussions, integrate disparate inputs, and reach a credible and appropriate decision.

8.1.2.3 Post Key Rollover Audit and Review

Every non-scheduled key rollover should be followed by a review of all aspects of the process:

- Was it carried out smoothly?
- Was it necessary?
- Was the decision process tuned to the threats?
- Was it fast enough but not overly fast?

- Was the information flow complete?
- Were appropriate procedures followed?

8.1.2.4 Reporting

Another requirement is for procedures for reporting and accountability to ensure transparency and credibility of the process.

8.1.3 Technology Evolution

Key management lives in a changing environment. Technological changes in both cryptography itself and computational resources require constant reevaluation of the technology used to create and manage the keys. For example, it is expected that an initial key length of 2048 bits is adequate and appropriate for the next several years. However, at some point, it might be necessary to shift to a longer key. Alternately, the current technology is based on the RSA algorithm. However, at some point, elliptic curve cryptography (ECC) might need to be adopted. Additionally, transition paths from one algorithm to the next will need to be decided upon.

These possible transitions generally take a long time to decide upon and will not depend solely on the resources within the RKO. However, it is vital that the RKO have the requisite resources to participate in such discussions, evaluate developing technologies, formulate plans and tests, and initiate technology transitions as appropriate.

8.1.4 Communication

Adequate reporting and transparency are important to maintaining the credibility of the process. For example, when a new RRset (for the keys) or a new public-private key pair is created, those events should be visible and publicized for the community to see and compare with the rest of the operation of the Root Zone. Similarly, there are likely to be queries from multiple sources, government and public, which require answers on a timely basis.

8.1.5 Policy and Legal Framework

The RKO will likely come into existence with a best efforts approach toward oversight, transparency and support. All of these are likely to evolve over a period of time. Accountability will also evolve over time. The degree of transparency and the specific information to be provided to various communities will need to change.

8.1.6 Finance

Finally, the financial support for this organization will be a continual source of concern. We do not make specific suggestions as to how the RKO will be funded but we do expect that both the sources and amounts of funding will change over time. The processes and organizational structure will have to evolve in response.

8.2 Organizational Structure

The staffing structure includes technical staff, management, and specialized functions (communications, legal, financial, etc.). These are detailed in the following paragraphs.

8.2.1 Technical Staff

Requirement for technical staff fall into three categories:

- Operational
- Development
- Strategic

Operational: The operational staff includes those who operate the key-management system. We assume that the staff will be on call 7 days a week, 24 hours per day.

Development: Responsibilities for the Development unit include: procurement of hardware and software, configuration of machines and systems, development of changes to processes, testing and documentation. For example, the initial configuration of facilities might consist of two Linux systems, growing within three years to specialized hardware in three redundant locations. Development staff would oversee and implement all of this work including growth in facilities and capabilities.

The implications relative to the two types of organizational options are substantial. Under the new unit options (1 and 2), the operational staff might be combined with the development staff since calls on their time from an operational perspective are likely to be infrequent. Under the existing unit options (3 and 4), however, operational duties might be assigned to existing staff who might already be performing similar functions and the development staff would be maintained as a separate group.

Strategic: The strategic staff carries out the following: monitoring developments in the technology, participating in community-wide discussions, and preparing the major decisions involving design and changes in technology. The strategic staff will also play an important role in communicating the technical structure and foundation of the RKO. The strategic function is segregated from development and operations to allow it to proceed without interfering with development and operations activities. This work may also involve considerable travel. When there are decisions to be made about key rollover, the chief strategic technical officer would be directly involved, as would the chief of operations.

8.2.2 Administrative Staff

Head office/central administration functions and roles include:

- Section/Unit Chief
- Administrative (accounting, human resources, comptroller, visitor control, security)
- Communications
- Legal
- Policy
- Finance

8.2.3 Committee of Visitors

A Committee of Visitors may be a viable strategy to enable transparency with concerned communities. Staff support will be required to coordinate this activity, with input from communications, technical, legal, and others.

The committee will be composed of public persons who are reputable and trusted with regard to Internet technologies and Internet security issues. This committee will perform independent reviews that will provide the following:

- Transparent views into the process to ensure that the process is being performed as stated.
- A public view into the processes, by proxy.
- Vetting of the process.

8.3 Resources

8.3.1 Human Resources

Human resources requirements are summarized in Table 1.

Table 1: Human Resources Requirements by Function and Option

Role	Self-contained Unit (Options 1 & 2)	Unit in Existing Activity (Options 3 & 4)	
	New staff	New staff in new unit	Added to existing units
Section chief/agency head	2	2	
Administration (internal)	5	2	2
Communications	1	1	
Legal	1		0.5
Policy	1		0.5
Finance	1		0.25
Technical – Development	6	4	
Technical – Operations	Part of Dev staff		1
Technical – Strategic	3	3	
Subtotal	20	12	4.25
TOTAL	20	16.25	

8.3.2 Facilities

Facilities span space and support for the staff, operations, and redundancy.

Operations facilities: The key generation and key signing equipment should be housed in a secured, protected facility that provides a level of security sufficient to remove all concerns about the protection of the systems.

External operations: External operations consist of room and some equipment for management, monitoring the health of the boxes that are housed in secure facility.

Equipment: The specific equipment and related costs are dependent on the technology options and, to a limited extent, on the architectural options.

Staff Facilities: In the first year, we envision an office at a single site. In the second year, it may be desirable to establish a second location in another part of the country.

9 Conclusion

This draft presented various options to realize the signing of the DNS Root Zone to facilitate DNSSEC deployment across the Internet. These options try to minimize changes to the existing process flow for maintaining the Root Zone, while providing secure mechanisms to sign and maintain a signed Root Zone. A signed Root Zone and a widely deployed DNS system that supports DNSSEC will be a major step forward in the ongoing effort to secure the Internet.

References

[1] Federal Information Processing Standards Publications (FIPS PUBS), http://www.itl.nist.gov/fipspubs.

[2] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[3] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[4] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[5] Eastlake, D., Brunner-Williams, E., and B. Manning, "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 2929, September 2000.

[6] Gudmundsson, O., "Delegation Signer (DS) Resource Record (RR)", RFC 3658, December 2003.

[7] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

[8] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[9] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[10] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[11] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.

[12] Kolkman O., and R. Geiben, "DNSSEC Operational Practices",

draft-ietf-dnsop-dnssec-operational-practices-06.txt (work in progress), October 2005.

[13] OpenSSL – Open Source Cryptographic Library, http://www.openssl.org

[14] OpenSC – Open Source Smart Card Library, http://www.opensc.org

[15] OpenCT – Open Source Smart Card Driver, http://www.openct.org

[16] NIC-SE DNSSEC Tools – pkcs15-dnssec keyset signer, http://dnssec.nic.se/sc

[17] BIND – Berkeley Internet Name Domain, http://www.isc.org/sw/bind

[18] Authoritative Name Server (ANS) from Nominum, http://www.nominum.com/products.php?id=2

[19]PGP Desktop from PGP Corporation, http://www.pgp.com/products/desktop/index.html

[20] DNSSEC-Tools, http://www.dnssec-tools.org

[21] Secure Zone Integrity Checker from NIST, http://www-x.antd.nist.gov/dnssec/

[22] nShield Hardware Security Module from nCipher,

http://www.ncipher.com/cryptographic_hardware/hardware_security_modules/8/nshield

[23] RSA BSAFE from RSA Security, http://www.rsasecurity.com/node.asp?id=1202

[24] SSH Tectia Solution for secure file transfer, http://www.ssh.com/products/tectia/

[25] Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

[26] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

[27] Perl Security and Encryption Modules, http://www.cpan.org/modules/by-category/14_Security_and_Encryption/

[28] National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for* Federal *Information Systems*, February 2005.

[29] National Institute of Standards and Technology Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006.

[30] National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, August 2005.

[31] Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

[32] Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

[33] Shinkuro secure file sharing from Shinkuro, Inc. http://www/shinkuro.com

Appendix A: Glossary

Term	Description
Auditor	An entity that performs audits of the edits to the Root Zone.
Content Audit	The function of auditing the changes to the contents of the Root Zone.
DNS	Domain Name System.
DNSSEC	Domain Name System Security Extensions.
IANA	Internet Assigned Numbers Authority. It accepts changes to the contents of the Root Zone from the TLD operators.
Key Audit	The function of auditing the changes to the Root Keyset and the signature over the Root Keyset.
Root Key Operator (RKO)	An entity that performs the function of generating the Root Zone's Key Signing Key (KSK) and signing the Root Keyset using the KSK. It may also perform generation of the root's Zone Signing Key (ZSK).
Root Key Signing Key (KSK)	The top-level key for the entire DNS hierarchy. DNS resolvers will configure the public portion of the KSK as a trust-anchor to validate signed DNS responses.
Root Name Server / Root Server	A DNS name server that serves the Root Zone. At present there are 13 Root Name Servers, named A through M, serving the Root Zone.
Root Server Operator (RSO)	An entity that operates a Root Name Server.
Root Keyset	A set of keys consisting of the Root Key Signing Key and the Root Zone Signing Key(s).
Root Zone Distributor (RZD)	An entity that performs the function of taking the zone file from the RZM and distributing it (or making it available) to the Root Servers.
Root Zone Maintainer (RZM)	An entity that performs the function of receiving changes to the Root Zone from the Auditor, storing the content of the Root Zone and generating the Root Zone file from this data. When Root Zone signing is introduced, the RZM will also be responsible for signing the contents of the Root Zone using the root's Zone Signing Key.
Root Zone Public Key	Refers to the public key of the root's KSK.
Root Zone Signing Key (ZSK)	The key used to sign the contents of the Root Zone.
TLD Operator	A Top-Level Domain Operator.
Trust Anchor	The public portion of a DNS key for a zone that is trusted to be authentic by a DNS resolver. In the context of the Root Zone, this will be the public portion of the Root Key Signing Key.

Appendix B: Mapping of Functions to Organizations

This document used functional names for various entities involved in the root-signing process. The following table lists the actual organizations currently performing the respective functions as well as the new functions that will need to be filled in by organizations.

Function	**Organization**
IANA	ICANN
Content Authorization	U.S. Department of Commerce
Key Audit	New Function
Root Key Operator	New Function
Root Zone Maintainer	VeriSign
Root Zone Distributor	VeriSign

Appendix C: Considerations for Multiple RKOs

The architectural options presented in Section 5 use a single RKO for generating the Root Zone's Key Signing Key. The advantage of using one RKO is that it represents a single incremental change to the existing process that is used for maintaining and changing the content of the root zone. There is a single entity that the RZM must communicate with and, once the appropriate security mechanisms are in place, the interactions between the two entities are generally unvarying.

It is also possible to use multiple RKOs in the Root Zone signing procedure. One possible approach uses a cryptographic approach known as" key-splitting" where each RKO will have a share of the key. This approach introduces explicit interdependencies to the process that should be avoided.

Another more robust approach is where each RKO is responsible for generating a distinct Root Zone KSK. The RKOs are themselves coequal such that temporary periods of outage suffered by one or more RKOs do not affect the overall functioning of the system as long as one RKO is unaffected. Multiple RKOs makes the architecture more resilient against temporary outages that might be suffered by a single RKO. It also allows for distribution of control over the Root Zone KSK amongst multiple entities which is desirable from the viewpoint of a decentralized Internet.

However, increasing the number of RKOs also increases the number of attack vectors in the root signing architecture. From the view of the DNSSEC validator, all KSKs for the root zone are equal; hence, if any of the RKOs are compromised, the entire root zone is also compromised.

Additionally, in order to support multiple RKOs, the RZM needs to implement two new functional elements: constructing the Root Keyset from the constituent ZSKs and KSKs; and constructing a "merged" signed zone from a number of other signed zones sent by RKOs using different zone signing keys. Of these, the first element is required when supporting multiple RKOs for any of the options presented in Section 5. The second functional element is required only to support Option 3 as specified in Section 5.3.

In order to maintain clarity, the multiple RKO approach is described under two different sub-sections: one with respect to the changes required in Options 1 and 2 (Section 5.1 and 5.2), and the other with respect to the changes required in Option 3 (Section 5.3). All of these changes affect only the Root Zone Maintainer and Root Key Operator blocks, so only these entities are shown in detail in the figures below. Since the process of requesting and authorizing changes to the content of the root zone through IANA remain unchanged, the TLD operator block, the IANA block, and the "Content Authorize" functional element within the Auditor block are not shown.

Appendix C.1: Multiple RKO Architecture for Options 1 and 2

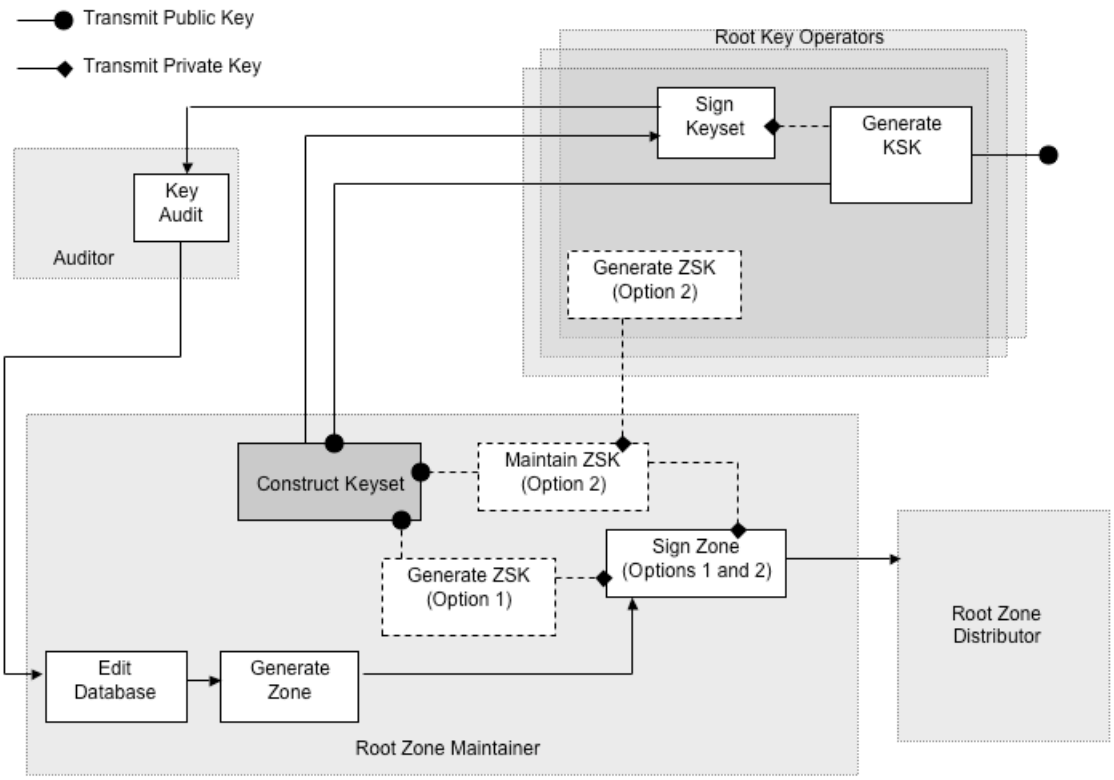

Figure 6: Multiple RKOs

Individual RKOs generate their own KSK and securely transmit the public key to the "Construct Keyset" block within the RZM. Without explicit coordination, the RKOs can not generate the Root Keyset individually; therefore, the RZM collects the input and constructs the Root Keyset. This step is essential since the signed Root Keyset has to be computed over the complete set of keys associated with the Root Zone which includes the public key portion from the KSKs from all of the RKOs. ZSKs for the Root Zone may either be generated at the RZM (Option 1) or at the RKOs (Options 2 and 3). Public keys from the "Generate ZSK" process must similarly be fed into the "Construct Keyset" functional block for creation of the complete Root Keyset. The transfer of public key information from the RKOs to the RZM must be over trusted channels that provide authentication, data integrity, non-repudiation, and possibly delivery assurance.

After the complete Root Keyset has been constructed, this information is securely transmitted to each of the RKOs for creating a signed Root Keyset using their respective Root Zone KSK. The transfer of this information from the RZM to the RKOs must be over a trusted channel that provides authentication, data integrity, non-repudiation, and possibly delivery assurance. Each RKO sends its respective signed Root Keyset to the Key Audit function for authorization and subsequent inclusion by the RZM into the Root Zone.

The "Sign Zone" operation is carried out within the RZM. The single signed root zone created from this process is sent to the RZD for distribution to the different Root Name Servers.

Appendix C.2: Multiple RKO Architecture for Option 3

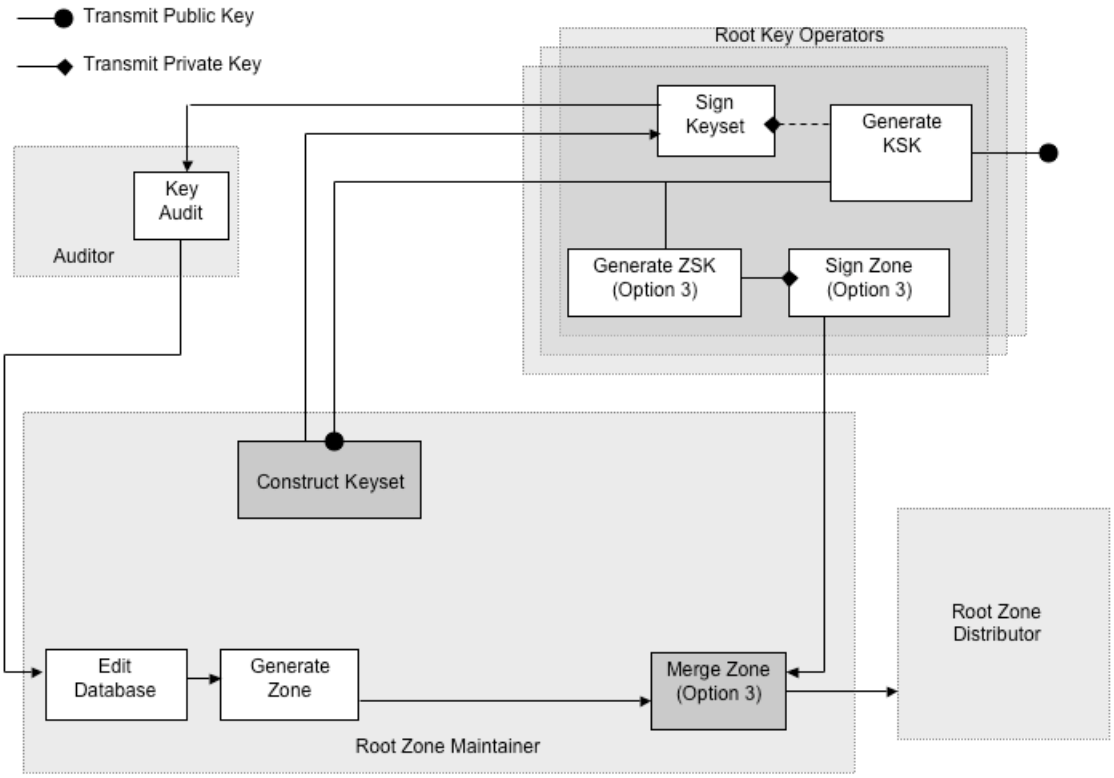

Figure 7: Multiple RKOs Option 3

Individual RKOs generate their own KSK and securely transmit the public key to the "Construct Keyset" block within the RZM. This step is essential since the each Root Keyset signature has to be computed over the complete set of keys associated with the Root Zone which includes the public key portion of the KSKs from all RKOs. ZSKs for the Root Zone are also generated at the RKO and must similarly be fed into the "Construct Keyset" functional block for creation of the complete Root Keyset. The transfer of public key information from the RKOs to the RZM must be over a trusted channel that provides authentication, data integrity, non-repudiation, and possibly delivery assurance.

After the complete Root Keyset has been constructed, this information is securely transmitted to each of the RKOs for creating a signed Root Keyset using their respective Root Zone KSK. The transfer of this information from the RZM to each of the RKOs must be over a trusted channel that provides authentication, data integrity, non-repudiation, and possibly delivery assurance. Each RKO sends its respective signed Root Keyset to the Key Audit function for authorization and subsequent inclusion by the RZM into the Root Zone.

In Option 3, the "Sign Zone" operation is carried out within the RKO. With multiple RKOs, each RKO creates a signed root zone using the ZSKs that it had itself previously created. The RZM receives the signed zone file from each RKO over distinct trusted channels that provide authentication, data integrity, non-repudiation, and possibly delivery assurance. The RZM then performs a "Merge Zone" operation, which is essentially the generation of the collective sum of all signed record sets in the zone with proper domain name ordering and duplicates removed.

The single signed root zone created from the "Merge Zone" functional block is sent to the RZD for distribution to the different Root Name Servers.

Appendix C.3: Number of RKOs

There are practical limitations on the number of RKOs that can be effectively supported within the Root Zone. The number of RKOs that can be effectively supported is influenced by the number of keys in the Root Keyset, the number of keys used to generate signatures for zone data, the key algorithm and key size, the message size that a typical response must fit within, and the architectural approach used from Section 5.

The following table lists the response size requirements for different numbers of ZSKs and KSKs for a query of the DNSKEY resource record type. The response sizes are calculated for a "minimal response" where no records are returned in the authority or additional sections of the DNS response, and with the assumption that the Root Keyset has only been signed with the Root KSKs (and not with the Root ZSKs).

Table 2: Keys to Message Size Requirement

	No. of KSK (Size: RSA 2048)	No. of ZSK (Size: RSA 1024)	Message Size
RKO generates only KSKs (Option 1)			
	8	2	4780
	6	2	3660
	6	5	4092
RKO generates KSKs and ZSKs; RZM generates no keys (Options 2 and 3)			
	6	6	4236
	4	4	2828

The following observations can be made:

- Option 1 supports 3 RKOs assuming above listed key sizes and effectively supports a maximum message size of 4096.
- Options 2 & 3 supports 2 RKOs assuming above listed key sizes and effectively supports a maximum message size of 4096
- The process of KSK rollover requires multiple KSKS to be simultaneously published. Since each RKO may be simultaneously rolling over its own KSK, the number of RKOs that can be effectively supported is half the number of KSKs listed in the above table.
- For Options 2 and 3 since the RKO is also responsible for generating the ZSK and different RKOs are themselves co-equal, in order to maximize the number of RKOs the number of ZSKs and KSKs must be equal.