DNSSEC Infrastructure Audit Framework

NLnet Labs Document 2013-002 Version 1.0

by Matthijs Mekking (matthijs@NLnetLabs.nl) and Olaf Kolkman (olaf@NLnetLabs.nl)

Abstract

This document describes a framework under which to conduct a review or audit of the DNSSEC related aspects of a registry and authoritative DNS name server service operation.

Table of Contents

1 Introduction

A DNSSEC audit is the process of structural examination of a DNSSEC infrastructure. The purpose of this process is to evaluate the level of assurance of the system. This is achieved by reviewing the implementation and operation of the system controls and whether they are in compliance with the corresponding policy requirements or, in absence of formal policies, with best current industry practices.

A key document for performing an audit is a review checklist. The review checklist provides structure of the actual work and gives confidence that the audit scope is adequately covered. This document is a generic checklist for a DNSSEC review and provides a framework that assists auditors to perform an actual DNSSEC audit. However, the actions herein do not conform any formal audit standards and are merely intended to provide directions of how an audit might look like.

This document is neither standard nor best practice and is not suitable for any form of formal certification. Its intention is to offer a basis for a structured review of a DNSSEC environment.

The authors welcome feedback on this document so that it can mature. The licensing terms of the document are such that any entity may modify and publish the document on their own terms as long as NLnet Labs is being acknowledged. Incorporation in other documents, including standards is encouraged.

1.1 Terminology

Readers of this framework are expected to be familiar with the DNS protocol [1][2], including its security extensions DNSSEC [3][4][5]. This document makes use of the terminology specified in RFC 2119 [6]. Furthermore, the following terms are being used:

- **Child Zone Manager**, the entity responsible for managing the child zone. This may be the registrant or the registrar, or a different party.
- **DNSSEC Policy (DP)**, a document that sets forth the requirements and standards to be implemented for a DNSSEC-signed zone.
- **DNSSEC Practice Statement (DPS)**, a document that describes how procedures and controls are implemented in order to meet the requirements from applicable policies.
- **Extensible Provisioning Protocol (EPP)**, a protocol for allocating objects within registries [7].
- **Hardware Security Module (HSM**), a system designed for private key generation and storage and accelerated creation of digital signatures.
- **Key And Signing Policy (KASP)**, a document that describes the timing and security parameters for signing zones.
- **Key Signing Key (KSK)**, a key for DNSSEC purposes that can be considered as a Secure Entry Point (SEP) and has the responsibility to sign the DNSKEY RRset.
- **(Domain Name) Registrant**, the entity that has registered a domain name.
- **(Domain Name) Registrar**, the entity that handles domain name registration requests and acts as the party between registrant and registry.
- **(Domain Name) Registry**, the entity that manages domain name registrations and operates the corresponding delegations.
- **Zone Signing Key (ZSK)**, a key for DNSSEC purposes that has the responsibility to sign all RRsets, except for the DNSKEY RRset.

1.2 Scope and Methodology

This DNSSEC audit framework is intended to be applicable to, but not limited to, top-level type domain registry and name server operations.

The main focus of this framework is on controls that preserve the integrity and availability properties of the DNSSEC related aspects of a DNS infrastructure and operation. As a consequence this document will not cover all aspects of a DNS registry operation but will touch on those aspects that are likely to influence the stability or security of the DNSSEC implementation and operation.

The methodology of this audit framework is loosely based on the ISO/IEC 27008:2011(E) Technical Report [8]. The scope is largely based on RFC 6841 [9], which covers an extensive list of topics that should be considered when implementing DNSSEC. Other deployment guidance can be found in the *Secure Domain Name System (DNS) Deployment Guide* from NIST [10][1].

For each section in this document we follow the following structure, loosely based on ISO/IEC 27008:2011(E):

Objective: Describes what the objectives of requiring a certain control are.

Control: Describes the control, which can metaphorically be seen as the knob that needs to be operated to reach the objective.

Practice:

Describes how the control can be realized, what the expected parameter space is. Or using the metaphor of the knob, the practice describes the type of knob (dial, switch) and what range of values are in its range. This part makes use of the RFC 2119 language, to set forth the implementation requirements.

Audit:

Describes what and how to check in order to assess that the control is properly implemented. Assessment checks take the form of

□ *Interviews:*

□ *One or more questions.*

□ *Examinations:*

□ *One or more verifications.*

□ *Tests:*

□ *One or more validations.*

Furthermore, the following assumptions are made:

During audit, it may be that controls that MUST or SHOULD be implemented are not implemented. A standard question that must be asked as follow-up is whether there has been a managerial decision, preferable documented, at the basis of the decision to not implement.

Some audits require to verify if controls meet the expected professional practices. What these expectations are, differ per control and are subject to the auditors perspective.

It may prove difficult to perform tests as an auditor if authentication and authorization mechanisms are in place. The framework assumes that a mystery account can be made available for such testing purposes.

[1] Caveat: this version of the document has not been reviewed against the NIST recommendations.

1.3 Preparations

1.3.1 Gathering Information

Auditors should prepare for the review by obtaining a general understanding of the organization, its operation, its system architecture and the controls that need to be reviewed.

This framework assumes the organization is a domain name registry, hereafter also referred to as registry or entity. In short, a registry manages domain name registrations and the technical operation of its own domains. Registration and delegation information is stored, where registration data is partially accessible through the WHOIS service and the delegation data is published in the DNS.

The following components are usually included in a DNSSEC enabled registry infrastructure:

- Registration portal, where registrars can register new domains, and update the delegation and public key information.
- Back-end database repositories, where administrative and technical information about domain name registrations and delegations are stored.
- DNSSEC signer, the part responsible for adding public key material to the entity's zone and digital signatures to the entity's zones resource records.
- Name servers, the machines responsible for handling DNS requests.
- Public registration data interface, more commonly referred to as WHOIS.
- Parent portal, where the registry can interact with the organization operating the parent zone (optional).

In order to familiarize themselves with the entity, auditors should get high level documentation or a general description of the implementation and availability of these components before the actual audit takes place.

The controls and objectives in this document are mainly based on RFC 2870: Root Name Server Operational Requirements [11] and RFC 6781: DNSSEC Operational Practices, Version 2 [12].

In addition to gaining knowledge about the entity, it is important to gather preliminary information from documents that are available from the registry already. Potential documentation includes:

□ Prior audit reports, if any.

□ DNSSEC Policy (DP) and Practice Statement (DPS).

□ Other policy documents and practice statements.

□ Internal operational documents.

It may be that these documents include sensitive information and the auditor is required to sign a Non Disclosure Agreement.

Finally, key personnel needs to be identified:

□ Senior Management (SM), responsible for managing the organization. They should be capable of identifying key personnel and know about personnel requirements.

□ Security Officer (SO), responsible for the organization's security. Responsibilities include implementing security processes, steering personnel in dealing with security processes, and responding to incidents.

□ Operations Management (OM), responsible for controlling the process of operation. They should set forth the business procedures.

□ System Administrator (SA), responsible for the operation of computer systems, like databases or network services. The role of SA can be divided over multiple persons each with its own expertise.

It is possible that these roles does not match well with the entity's organizational structure, but it is important to identify the responsibilities and the personnel who carries out these tasks.

1.3.2 Complexity of the Audit

ISO 27006:2011 [13] Appendix A provides some information on how to assess the entity’s risk potential in order to assess the audit complexity. Factors include number of employees, users, locations, servers, and workstations.

Further description of this type of analysis is out of scope for this document.

1.4 Outline

Section 2 describes audit actions that should be applied on documents, that preferably are already gathered before the actual audit. In section 3, facility and management controls are being covered. Section 4 looks closer to the domain name registration system and how child zone operators can submit their DNSSEC records. Sections 5, 6 and 7 handle technical security controls regarding name servers, key pairs, and network. Sections 8 and 9 cover zone signing and how this affects the zone contents. Section 10 covers logging controls. Section 11 lists some other controls that may be considered in a future version of this document.

2 Documentation

This section describes the controls for an entity to publish information regarding DNSSEC policies, practices and operations. For each document it is important to think about its accessibility and maintenance. A DNSSEC policy or practice statement may be used as the body of knowledge for a compliance audit.

2.1 Public Documentation

2.1.1 DNSSEC Policy and/or Practice Statement

Objective: Gain a shared understanding and transparency of choices and procedures for all stakeholders.

Control: Make the DP and/or DPS publicly available and accessible through the Internet.

Practice:

A DP(S) contains the relevant information for the stakeholders. In the case of a registry, this is typically the Internet community. The DP(S) SHOULD thus be easily accessible to the general public e.g. though publication on the entity's website.

The DP(S) SHOULD include all topics outlined in RFC 6841. Topics MAY require no stipulation, in those cases there should be a considered managerial decision at the basis of such choice.

The DP(S) SHOULD include an emergency contact method that describes how and where child zone managers can request an emergency key rollover.

The DP(S) SHOULD NOT include topics that could be considered sensitive details of the entity's operation.

There SHOULD be someone assigned with the responsibility of the maintenance and publication of the DP(S), for example the Security Officer.

Stakeholders SHOULD be enabled to keep up to date with changes of the DP(S), e.g. through mailing list, RSS feed, etc.

Audit:

□ *Interview: SO, OM.*

□ *Question: Does the entity publish a DP(S)?*

□ *Question: If there are topics in the DP(S) that require no stipulation, are those supported by management?*

□ *Question: Who is responsible for the upkeep of the DP(S)?*

□ *Question: How are stakeholders notified in case of changes in the DP(S)?*

□ *Examine: Publication mechanism of the DP(S).*

□ *Verify: The DP(S) is easy accessible.*

□ *Examine: The DP(S).*

□ *Verify: The document covers all topics outlined in RFC 6841.*

□ *Verify: The document includes information on the emergency contact method for child zone managers.*

□ *Verify: No sensitive information is being covered in the DP(S).*

□ *Examine: Notification mechanism of the DP(S).*

□ *Verify: The mechanism enable stakeholders to be kept up to date with changes in the DP(S).*

2.1.2 Trust Anchor Announcement

Objective: Allow for establishing trust in an out-of-band manner.

Control: Publish public key information out-of-band how to set up trust anchors for the entity's zone.

Practice:

There MAY be an out-of-band publication mechanism for SEP keys available, for example on the entity's website. If no out-of-band publication mechanism is available, there SHOULD be a specific statement that the public keys should not be used as trust anchors.

The out-of-band publication SHOULD have a security mechanism that ensures authenticity and integrity of the publications. This can be achieved by publishing the public keys on a SSL secured web site. Another option is to create a digital signature on the public keys with PGP.

Every out-of-band announcement of change in public keys or change of publication mechanism SHOULD be signed and verifiable by its own security mechanism.

Audit:

□ *Interview: SO, OM.*

□ *Question: Is there an out-of-band publication mechanism for SEP keys?*

□ *Question: How are announcements communicated to stakeholders?*

□ *Examine: The out-of-band publication mechanism.*

□ *Verify: The public keys published are identical to the public keys published in the DNS (either in DS or DNSKEY format), or there is a statement that the keys should not be used as trust anchors.*

□ *Verify: The security mechanism for communicating this information ensures message authentication and integrity.*

□ *Examine: An out-of-band announcement of change in public keys.*

□ *Verify: The security mechanism for communicating this announcement ensures message authentication and integrity.*

2.2 Internal Documentation

2.2.1 Business and Technical Procedures

Objective: Achieve business continuity through knowledge sharing between employees.

Control: Make business and technical procedures available for DNS operators.

Practice:

Business and technical procedures SHOULD be easy to find for the DNS operators. There is no requirement to make such procedures publicly available, but if they include sensitive information SHOULD NOT be publicly accessible.

There SHOULD be procedures describing the zone signing system, key generation and rollover and key compromise handling.

Audit:

☐ *Interview: OM.*

☐ *Question: Who is responsible for the upkeep of business and technical procedures?*

☐ *Question: How are DNS operators notified in case of changes in the documents?*

☐ *Interview: SA.*

☐ *Question: Is it known where business and technical procedures can be found?*

☐ *Examine: Business and technical procedures.*

☐ *Verify: The documents that are publicly available contain no sensitive information.*[2]

☐ *Verify: The documents are complete with respect to the DNSSEC operation of the entity.*

☐ *Examine: Publication location of business and technical procedures.*

☐ *Verify: There is access control on the documents.*

2.2.2 Incident Response Procedures

Objective: Allow for a quick recovery after a detected compromise or disaster, for example private key loss.

Control: Have provisions in place that can be followed to recover from a compromise or disaster.

Practice:

According to RFC 2870: “Provision MUST be made for rapid return to operation after a system outage. This SHOULD involve backup of systems software and configuration. But SHOULD also involve backup hardware which is pre-configured and ready to take over operation, which MAY require manual procedures.”

Furthermore, an incident response procedure SHOULD exist. This document SHOULD be easy to find and execute. The procedures SHOULD include an investigation to the root-cause of the incident. Procedures SHOULD include the process of recovering compromised data, systems, machines and mechanics. Procedures SHOULD include the way of reporting the incident.

Audit:

☐ *Interview: SO.*

☐ *Are there backups of data, systems software and configuration that allow for rapid recovery after a compromise or disaster?*

☐ *Examine: Incident response procedures.*

☐ *Verify: The documents that are publicly available contain no sensitive information.*

☐ *Verify: The documents are complete with respect to the DNSSEC operation of the entity.*

☐ *Examine: Publication location of incident response procedures.*

☐ *Verify: There is access control on the documents.*

2.3 Entity Termination

This section deals with controls when the entity stops DNSSEC support or entirely stops its operation.

[2] What is considered sensitive information is left to the auditors own devices.

2.3.1 Disabling DNSSEC

Objective: Allow relying parties to react and find other possible alternatives and provide for a smooth transition to alternative parties.

Control: Announce the event of disabling DNSSEC well in advance.

Practice:

Relying parties may be using functionality that requires DNSSEC (e.g. DANE). Such parties SHOULD be notified in advance so that they can rollover to possible other solutions.

In case of the entity discontinues operation, it SHOULD provide transparency by notifying stakeholders in advance and should cooperate with the transition to the new party.

3 Facility and Management

This component describes non-technical security controls that need to be considered when implementing DNSSEC. RFC 2870 [11] describes guidelines for operation of the root name servers, which are considered also applicable to registry name server operations.

3.1 Physical Controls

Physical controls are required to prevent intrusion and denial-of-service of machines that have a crucial part in providing DNS service. These controls are out of scope of this audit because they are not DNSSEC specific. However, these controls may become more important when implementing DNSSEC.

3.1.1 Geographical Diversity

Objective: Reduce the impact of a natural or IT disaster.

Control: Ensure that not all name servers are in the same physical location.

Practice:

At least one secondary name server SHOULD be hosted in a different location than the facility that is being audited.

3.1.2 Facility Architecture

Objective: The building that houses the registry and name server operation is sufficiently impossible to intrude.

Control: Use intrusion prevention and detection systems.

Practice:

The prevention and detection of intrusion is achieved by following physical security mechanisms, such as the use of strong locks and alarm systems.

There MAY be more buildings that houses registry and name server operation, to provide redundancy in case of geographical incidents.

3.1.3 Power Continuity

Objective: Achieve operational continuity in case of a power incident.

Control: Provide power fallback in case of a power outage.

Practice:

In case of an outage, power continuity for at least 48 hours SHOULD be assured.

This MUST supply the server itself, as well as the infrastructure necessary to connect the server to the Internet.

There SHOULD be procedures which ensure that power fallback mechanisms and supplies are tested no less frequently than the specifications and recommendations of the manufacturer.

The risk of power outages MAY be reduced by diversity in power grids.

3.1.4 Fire and Other Disaster Prevention

Objective: Achieve operational continuity in case of a fire incident.

Control: Have fire prevention mechanisms.

Practice:

RFC 2870 states that fire detection and/or retardation MUST be provided.

Besides fire, other natural disasters, for example flooding, tornados, or zombie outbreaks [14] may happen. The risks for such disasters differ per region.

3.2 Procedural Controls

Besides physical controls, procedural controls can be used to prevent intrusion of areas where machines are located that have a crucial part in providing DNSSEC service.

3.2.1 Area Access Control

Objective: Prevent intrusion in areas that house servers critical for business operations.

Control: Control access to areas where name servers and signers are located.

Practice:

The relevant areas MUST have positive access control.

The number of individuals permitted access to the area MUST be limited, controlled, and recorded.

Control measures SHOULD include either mechanical or electronic locks.

Physical security MAY be enhanced by the use of intrusion detection and motion sensors, multiple serial access points, security personnel, etc.

Audit:

□ *Interview: SO, OM.*

□ *Question: What area access control requirements do areas where the signing system and key storage are housed have and are those requirements documented?*

□ *Question: Who has access to those areas?*

□ *Question: How is access to those areas recorded?*

□ *Examine: Relevant areas.*

□ *Verify: The areas make use of mechanic or electronic locks.*

□ *Verify: Access to areas is logged.*

□ *Verify: If there are intrusion detection mechanisms in place.*

3.2.2 Trusted Roles

Objective: Have limited access to critical business operations

Control: Identify several trusted roles for certain operations.

Practice:

The entity SHOULD at least identify one person as the Security Officer (SO). The SO is responsible for the entity's security posture.

The entity SHOULD at least identify one person as the Systems Administrator (SA). The SA is responsible for the reliable operation of the computer systems.

For DNSSEC operations there should be explicit responsibilities with respect to the aspects of private and public key management.

Audit:

□ *Interview: SM.*

□ *Question: Is there someone that has the trusted role of SO?*

□ *Question: Is there someone that has the trusted role of SA?*

□ *Question: How are trusted roles identified and authenticated?*

□ *Question: Who is responsible for the DNSSEC aspects of the operation?*

3.2.3 Separation of Duties

Objective: Prevent unauthorized, fraudulent or unwanted actions by a single person.

Control: Require more than one person to perform critical procedures.

Practice:

The entity SHOULD have identified critical procedures that require multi-person access, for example key generation. The number of persons requires should be based on an assessment of the risks of collusion.

These procedures SHOULD be documented.

Audit:

□ *Interview: SO, OM.*

□ *Question: Are the risks of collusion understood?*

□ *Question: What procedures require multi-person access?*

□ *Question: Are these procedures documented?*

3.3 Personnel Controls

This section addresses controls in order to demonstrate trustworthiness and qualifications of trusted role candidates. These controls are out of scope of this audit because they are not DNSSEC specific, but again may become more important when implementing DNSSEC.

3.3.1 Personnel Requirements

Objective: Ensure that personnel is capable of performing their responsible actions and is trustworthy.

Control: Verify qualifications and trustworthiness of candidates.

Practice:

Candidates can demonstrate their qualifications and trustworthiness during the solicitation procedure. As part of the job offering, the entity MAY perform additional background checks, including the candidate's resume, employment history and education.

The job offering MAY include training to make the candidate familiar with the entity's organization, operation and ethical code.

3.3.2 Sanctions

Objective: Ensure that personnel is trustworthy and prevent damage to the entity's image.

Control: Have sanctions for unauthorized actions.

Practice:

There SHOULD be responsibility and confidentiality agreements that make clear which actions result in sanctions and what those sanctions are.

4 Domain Name Registration System

This section covers the domain name registration system and how child zone operators can submit their DNSSEC records. It does not exclusively deal with DNSSEC aspects of the operation, but takes a somewhat broader view.

4.1 Meaning of Domain Names

This section deals with child zone naming controls.

4.1.1 Domain Name Requirements

Objective: Prevent operational or legal problems because of semantics or syntactic content of domain names.

Control: Reject domain names that introduce legal, operational or technical havoc.

Practice:

There are no specific DNSSEC aspects to this control, however when domain names are registered that lead to operational or technical problems, that may also affect the DNSSEC operation. Therefor, this framework covers some implementation guidance for a domain name check.

There SHOULD be a policy document that lists the requirements for new domain name registrations. All kinds of checks are possible, for example whether the name is already delegated, whether the name is preserved, whether the name does not contain disallowed substrings. The reason to do this might be legal and/or operational, for example to prevent events such as typo squatting and brand hijacking.

There SHOULD be a tool that checks the registrations of domain names against the requirements. If checks cannot be automated, the checks SHOULD be performed manually.

Audit:

□ *Interview: OM.*

□ *Question: Is there a policy on domain name and resource record registration?*

□ *Interview: SA.*

□ *Question: If there is a policy on domain name and resource record registration, how are its requirements implemented?*

□ *Examine: The requirements set forth by the registration policy.*

□ *Verify: That technical and procedural controls are implemented to prevent operational or technical violations of the policy.*

□ *Test: The domain name registration system.*

□ *Validate: Technical controls as required by the policy have been implemented in the domain name registration system.*

4.1.2 Delegation Requirements

Objective: Provide trustworthy and stable DNS consistency for the entity and its delegation points, to reduce brittleness in DNS resolving.

Control: Perform a consistency check on delegations.

Practice:

Next to a domain name check, a zone check SHOULD be performed. A zone check SHOULD have some heuristic checks that can provide confidence that updates to the zone are correct. For example, it could examine the size of the entity's zone.

A zone check MAY examine how stable delegations are. There can be many things to check, such as the consistency of the NS RRset and Glue RRsets between the entity and the child, consistency of the SOA RRset, lameness of name servers, if name servers comply with certain guidelines (closed zone transfer, whether it can answer queries over UDP and TCP, ...), connectivity, and more.

The entity SHOULD perform additional DNSSEC checks. This MAY include whether the name servers do DNSSEC processing, whether the DNSKEY RRset uses sane parameters, if the DNSKEY RRset corresponds to the DS RRset, and more.

If checks fail, human intervention MUST be in place to resolve the problem and the failure SHOULD be logged.

Audit:

□ *Interview: OM.*

□ *Question: Is there a policy on zone content and parent to child delegation checks?*

□ *Interview: SA.*

□ *Question: If there is a policy on zone delegations and content, how are its requirements implemented?*

□ *Question: Is a DNSSEC check for delegations implemented?*

□ *Question: What happens if a check fails?*

□ *Examine: Documented or reported requirements for delegation checks.*

□ *Verify: Existence and reasonable (in terms of professional practice) requirements for the checks.*

□ *Test: The zone check mechanism.*

□ *Verify: The coverage of zone and delegation checks meet requirements and expected professional practices and covers important DNSSEC requirements.*

4.1.3 Identification and Authentication of the Registrar

Objective: Maintain trust by appropriate delegation and prevent 'hijack'.[3]

Control: Authenticate domain name registration applicant and authorize transactions.

Practice:

How the registrar requests new domain name registrations can be implemented in many ways, for example trough a web interface. The identification and authentication of the registrar is subject to general security mechanisms. This framework assumes that these general mechanisms are out of scope of a DNSSEC audit. Nevertheless, some general audit actions can be performed.

Audit:

□ *Interview: SO, SA.*

□ *Question: What security mechanism is used?*

□ *Question: Does the mechanism follow good guidelines with respect to password length, storage, cryptographic parameters, ...?*

[3] This objective is important when DNSSEC enables other applications to infer more trust from the DNS.

□ *Question: How are the initial authentication credentials distributed?*

□ *Question: Is there a recovery mechanism in case of an incident?*

□ *Question: How many unique points of contact are required/allowed per registration?*

□ *Test: Operational implementation of identification mechanism.*

□ *Validate: Whether operational implementation meets reported requirements and expected professional practices.*

□ *Test: Technical implementation of authentication mechanism.*

□ *Validate: Whether technical implementation meets requirements and expected professional practices.*

4.2 Identification and Authentication of Child Zone Manager

This section deals with how the child zone manager has initially been identified, and how subsequent requests are authenticated.

No stipulation. These tasks are considered to be the responsibilities of the registrar. In case that the entity is also accepting domain name registrations directly from registrants, the controls in section 4.1.3 can be reused.

4.3 Registration of Delegation Signer (DS) Resource Records

This section describes the controls for establishing the chain-of-trust to the child zones by retrieving and publishing DS Resource Records.

4.3.1 Acceptance and Storage

Objective: Maintain consistency and prevent alteration to the child public key material during the lifetime at the registry.

Control: Accept DNSSEC records in such a way that a chain-of-trust to the child zone can be created or remains intact – maintain a chain of custody.

Practice:

The entity is RECOMMENDED to accept DNSKEY records, in order to be able to roll to a different digest type in the future, or to be able to provide aid to the Registrant in the case of a DNS Operator change.

The entity MAY accept DS records, in case of child zones that want to have a DS published using a message digest algorithm not understood by the entity. If the entity wants to allow for rapid change of used digest algorithms (without requiring actions from the child zone managers) to be prepared for discovery of cryptographic weaknesses, the DNSKEY SHOULD be attached in the DS submit request. The entity MAY query for the DNSKEY RRset for the child zone and make sure it matches, but should be aware that there are valid reasons for submitting a DS that does not match any externally visible DNSKEY record.

The initial key exchange SHOULD be authenticated and authorized at least as strong as the authentication and authorization mechanisms used for the exchange of delegation information (NS and Glue records).

Audit:

□ *Interview: SA.*

□ *Question: In what format is Delegation Signer data accepted and stored?*

□ *Examine: In what format Delegation Signer records are accepted and stored.*

□ *Verify: Delegation Signer data in DNSKEY (or DS) format is accepted and stored as such.*

□ *Examine: The security mechanism for Delegation Signer registration.*

□ *Verify: It is at least as strong as the mechanism for exchanging NS and Glue records.*

□ *Test: The Delegation Signer registration mechanism.*

□ *Validate: Delegation Signer data can be submitted in DNSKEY (or DS) format.*

4.4 Method to Prove Possession of Private Key

This section describes how the child zone manager should provide proof of possession of the private key that corresponds to the current or any successor Delegation Signer information, to ensure that published DS records can actually be used to build the chain-of-trust between the entity and the child zone. This can for example be achieved by requiring self-signed keys to be included when Delegation Signer records are being registered.

No stipulation. These tasks are considered to be the responsibilities of the registrar.

4.5 Removal of DS Resource Records

This section covers the controls for when a registrant wants to go back to unsigned.

4.5.1 Procedure for Removal of the DS RRset

Objective: Prevent a degrade of security in the delegation.

Control: Request an acknowledgement to make the child zone insecure from the registrant, or the party authorized by the registrant.

Practice:

There MAY be a procedure that describes who is allowed to acknowledge the removal of a delegation DS RRset.

The communication channel SHOULD have a security mechanism that ensures authenticity and integrity of the acknowledgement. For example, EPP provides an additional mechanism, the Domain Name Password (EPP authInfo), which can be used by registries to authenticate a registrant.

Audit:

□ *Interview: SO, SA.*

□ *Question: Is there a procedure for complete removal of the DS RRset?*

□ *Examine: The procedure for removal of the DS RRset.*

□ *Verify: Only the registrant or the party authorized by the registrant can acknowledge a request complete removal of the DS RRset.*

□ *Test: The mechanism for removal of the DS RRset.*

□ *Validate: The mechanism provides authentication and integrity.*

4.6 Removal or Transfer of Domain Name

Domain names may be removed or transferred to a different DNS operator or registrar. This section covers these scenarios. This control is not DNSSEC specific, but unauthorized changes to the domain name may impact the DNSSEC operation of that domain name.

4.6.1 Procedure for Removal or Transfer of Domain Name

Objective: Prevent unauthorized or unwanted changes to the domain name, domain hijacking.

Control: Have mechanisms in place to prevent unauthorized or accidental changes to the domain name.

Practice:

The entity SHOULD implement precautions which prevents a registry from modifying or transferring a domain name unless the corresponding registrar removes the lock, for example with a Registrar-Lock.

The entity SHOULD also support a five-day transfer pending period, during which the registrar can verify the transfer with the registrant.

The entity SHOULD support a mechanism to authenticate the registrant, for example with EPP Domain Name Password mechanism (EPP authInfo).

Audit:

□ *Interview: SA.*

□ *Question: Is a Registrar-Lock or are similar precautions implemented?*

□ *Question: Is a five-day transfer pending period implemented?*

□ *Question: Does the procedure support a mechanism to authenticate the registrant?*

□ *Test: The technical implementation of the Registar-Lock.*

□ *Validate: The entity cannot make changes to the domain name when the Registar-Lock is set.*

□ *Test: The transfer pending period.*

□ *Validate: In case of a transfer of domain name, there is pending period before the actual changes are being committed.*

5 Name Servers

This section handles all kinds of computer security controls, such as access control, how to cope with errors, and more. These controls are not DNSSEC specific, but the lack of good computer security controls may threaten the healthiness of a DNSSEC operation. These controls can also be applied to key signing systems, terminals, etc.

5.1 Secure DNS Instances

Objective: Prevent and detect unwanted access to machines that are critical for the entity's operation.

Control: Secure the DNS related systems.

Practice:

The operating systems SHOULD run the latest versions, so that all fixes to known vulnerabilities have been installed.

The name servers SHOULD NOT trust other hosts, except secondary servers trusting the primary server, for matters of authentication, encryption keys, or other access or security information.

The name servers MUST NOT rely on address or name-based authentication.

The name servers themselves MUST NOT provide services other than the authoritative name service, with a few exceptions:

□ Servers SHOULD have a secure mechanism for remote administrative access and maintenance.

□ Servers SHOULD be able to act as a Network Time Protocol (NTP) client [15].

There should be a minimum of roles that have access to the DNS related systems. The roles that have access to these systems SHOULD be documented. The level of access control may be different for name servers, signing systems, database repositories, etc.

Audit:

□ *Interview: SA.*

□ *Question: What are the policies to maintain operating systems?*

□ *Question: How do system security announcements reach you in a timely manner?*

□ *Question: Who is able to access the name servers and other DNS-related systems?*

□ *Question: How is access control implemented on these systems?*

5.1.1 Secure DNS Software

Objective: Minimize vulnerabilities and impact of vulnerability exploitation in DNS software.

Control: Maintain a modern and up-to date implementation with well understood configuration.

Practice:

A modern implementation SHOULD be used and its configuration should be well understood. This includes running the latest versions of the software, with restricted privileges and limited services.

The entity SHOULD be subscribed to vendor security announcement lists and track vulnerabilities announcements by computer security incident response teams.

Fingerprinting of the implementation SHOULD be prevented in order to defer zero-day exploits.

Audit:

□ *Interview: SA.*

□ *Question: What are the policies to maintain the DNS software?*

□ *Question: How are name servers configured to run, with respect to privileges and services (e.g. are name servers configured to use recursion)?*

□ *Question: How do DNS security announcements reach you in a timely manner?*

□ *Question: How is configuration of name servers managed?*

□ *Test: Rudimentary fingerprinting: 'dig CH version.bind|server.id TXT'*

□ *Validate: Name servers cannot be identified by fingerprinting.*

5.1.2 Diversity in Systems

Objective: Reduce the impact of hardware and software bugs.

Control: Use different hardware and software for systems that are used as name servers.

Practice:

Name servers SHOULD have different hardware.

Name servers SHOULD be ran from different operating systems.

Name servers SHOULD be using different name server implementations.

Audit:

□ *Examine: Name servers.*

□ *Verify: Name servers vary in used hardware.*

□ *Verify: Name servers vary in used operating systems.*

□ *Verify: Name servers vary in used implementations.*

5.1.3 DNSSEC Processing

Objective: Provide reliable DNSSEC answers to validators.

Control: DNSSEC enabled authoritative name servers.

Practice:

All authoritative name servers must offer the features on which the zone relies.

All authoritative name servers MUST include the appropriate RRSIG, NSEC (or NSEC3) and DS records when the DO bit is set in the query.

All authoritative name servers MUST clear the CD bit when composing the authoritative response.

All authoritative name servers MUST clear the AD bit if the response is a referral.

Audit:

□ *Interview: SA, OM.*

□ *Question: How is assurance provided that all authoritative name servers comply to appropriate specifications?*

□ *Test: Query all authoritative name servers for existing and non-existing data.*

□ *Validate: All servers return responses with expected DNSSEC resource records.*

□ *Validate: All servers set the DO bit and clear the CD bit.*

□ *Validate: All servers clear the AD bit in case the response is a referral.*

5.2 Zone Replication

The entity's zone stored in a back-end repository must be transferred to multiple (secondary) name servers. Having multiple name servers provides the entity with a better redundancy and capacity to improve the performance of handling DNS requests.

5.2.1 In-band Replication

Objective: Allow for (incremental) zone replication between name servers.

Control: Transfer entity's zone to multiple servers using the DNS.

Practice:

There SHOULD be a minimum of two (but preferably more than two) public accessible name servers that serve the entity's zones.

Name servers SHOULD support AXFR, IXFR and NOTIFY mechanisms in order to achieve in-band zone replication.

Name servers SHOULD support TSIG and IP address based ACL to allow zone transfers between the entity's servers exclusively.[4] How the ACL is designed depends on the infrastructure. For example, in the case of a hidden primary, the zone transfer flow in one direction. In case of a mesh, each entity's server is allowed to request and serve zone transfers.

TSIG keys SHOULD be of sufficient strength (112 bit) and randomly generated and be unique to each entity that is interacted with.

TSIG keys should be handled securely. That is, after creation of the secret, the transmission to the name servers SHOULD provide integrity and confidentiality.

The TSIG keys SHOULD be configured separately from the name server configuration file, most likely with different permissions.

The REFRESH parameter in the SOA Resource Record determines the frequency of zone transfers when no NOTIFY is being received. It SHOULD be set to a sane value that corresponds to SLA regarding how fast updates in the zone are visible.

The RETRY parameter in the SOA record determines when a zone transfer request should be send in case a previous attempt failed. This value SHOULD be lower than the REFRESH value, so that at least a couple of retries can be made before the next refresh timer expires.

The controls for the EXPIRE parameter are covered in section 9.2.3.

Audit:

□ *Interview: SO, SA.*

□ *Question: What is the strength of the TSIG key and how is the key generated?*

□ *Question: How are TSIG keys shared e.g. are they unique to each entity?*

□ *Question: How are TSIG keys used and maintained e.g. file permissions, storage, backup.*

□ *Question: How are TSIG keys distributed towards the name servers?*

□ *Examine: The SOA record.*

[4] This guidance is convoluted with a privacy control. It is assumed that there is a requirement that the zone data is not publicly available as a zone transfer.

□ *Verify: The values for REFRESH and RETRY are sane.*

□ *Examine: Name server configuration files.*

□ *Verify: Both name servers that are involved in a transaction have the same TSIG key configured, so that both the request and the response are signed.*

□ *Test: The authoritative name servers.*

□ *Validate: Support of AXFR, IXFR, NOTIFY.*

□ *Validate: Zone transfers are closed for non-authoritative sources.*

□ *Validate: There are two or more name servers that serve the entity's zones.*

5.2.2 Out-of-band Replication

Objective: Allow for zone replication in case of a critical network failure or in case of a denial of zone transfer.

Control: Have in place out-of-band methods to transfer entity's zone to (secondary) name servers.

Practice:

Each server SHOULD have a method to update the zone data via a medium which is delivered through an alternative path, possibly other than DNS, e.g. through rsync. In other words, there should be a fallback mechanism to perform zone replication, in case normal operations fail.

Audit:

□ *Interview: SA.*

□ *Question: How is out-of-band zone replication realized?*

6 Key Pair Handling

This component describes the technical security controls with respect to DNSSEC related cryptographic keys and activation data. This covers key generation, authentication, registration, auditing, archiving, and protection.

6.1 Key Pair Generation and Installation

This section deals with controls related to the key pair generation and installation.

6.1.1 Key Pair Generation

Objective: Generate secure and trustworthy keys required for DNSSEC operation.

Control: To generate keys, use systems that provide transparency, and are able to generate good randomness.

Practice:

There SHOULD be a key generation procedure document that lists the requirements and tasks with respect to key pair generation. This can include the trusted roles that are required for key generation, what systems are to be used, if there are n-out-of-m controls applicable, etc.

The physical key generation SHOULD be performed on a HSM, which provides reasonable assurance that keys are generated in a secure manner with respect to the generation of random bits, and with respect to checks on other important key parameters such as the used prime numbers and exponent size. If no HSM is used for the key pair generation, the system SHOULD have its own mechanisms to ensure good randomness and to perform key parameter checks. Technical suggestions for the generation of random keys can be found in RFC 4086 [16] and NIST SP 800-90A [17][5], amongst others. The examination of that specific system is out of scope for the purpose of this audit framework.

The whole procedure SHOULD be logged to an external system to produce an audit-trail of the event. These audit-trails SHOULD include personnel involved, software versions used, and time of generation.

Audit:

□ *Interview: SO, OM.*

□ *Question: Is there a document that describes the key generation procedures?*

□ *Examine: The key generation system.*

□ *Verify: The system is a HSM or an alternative signing system that provides the generation and storage of private keys in a secure manner.*

□ *Examine: Logs of the key generation.*

□ *Verify: Key pair generation events have been logged.*

□ *Verify: The event log is complete and contains involved personnel, software versions used, and timings.*

□ *Verify: Exceptions are being caught and acted upon.*

6.1.2 Public Key Delivery

Objective: Ensure that the public key component exported to the entity's zone is authentic.

Control: Verify the integrity of the public key component during the export from the key generation

[5] 800-90A is currently under review. See http://csrc.nist.gov/news_events/index.html#sept24

system to the entity's zone.

Practice:

There SHOULD be one or more trusted roles that verifies the integrity of the public key component after export, for example the SO and/or the SA. The same roles SHOULD be responsible for the publication of the key, and the verification that the key is properly propagated towards the secondary servers.

Audit:

□ *Interview: SO.*

□ *Question: How is integrity verification on the public key component realized?*

6.1.3 Key Usage Purposes

Objective: Reduce the damage in case of a key compromise.

Control: Have separation of duties for keys.

Practice:

Keys that are used for the purpose of DNSSEC SHOULD not be used for any other purpose.

The signing system SHOULD not be used for other purposes other than DNSSEC.

Audit:

□ *Interview: SO.*

□ *Question: Does the entity use keys for other purposes than DNSSEC?*

□ *Question: For each used key pair, what are its purposes?*

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Controls for private key protection and cryptographic modules need to be in place for key generation and creation of signatures.

6.2.1 Private Key Storage

Objective: Prevent unwanted exposure and/or modification of private keys.

Control: Store private keys in a secure manner.

Practice:

The private keys SHOULD be stored in FIPS-140-2 or similar certified systems. Its security level SHOULD be level 2 or similar level.[6]

Private keys MUST NOT be stored in other places other than the system designed for private key storage.

For extra security, private keys MAY be stored off-line, although this poses additional operational complexity.

Audit:

□ *Interview: SO.*

□ *Question: What systems are being used for private key storage?*

[6] The examination of the system itself and whether it is FIPS-140-2 or like compliant is out of scope.

□ *Question: Can private keys be exported from the system?*

□ *Question: What certification applies to the system?*

6.2.2 Private Key Backup

Objective: Provide a way to recover from private key loss.

Control: Backup private keys to a different system.

Practice:

When choosing a storage medium, possibilities of backup of its data should be examined. Of course, these backups SHOULD have the same protection as the original, if not more.

Audit:

□ *Interview: SO.*

□ *Question: When are backups of private keys performed?*

□ *Question: To what system is the backup made and what certification applies to the backup system?*

6.2.3 Private Key Activation

Objective: Prevent unwanted usage of the private key.

Control: Use activation mechanisms on the private key.

Practice:

There SHOULD be a trusted role that is able to activate the key. There MAY be m-out-of-n controls for key activation.

Activation SHOULD have a proper authentication mechanism in place, for example two-factor authentication.

Audit:

□ *Interview: SO.*

□ *Question: Who has authorization to activate keys?*

□ *Question: How are keys activated?*

6.2.4 Private Key Deactivation

Objective: Prevent unwanted usage of the private key.

Control: Use deactivation mechanisms on the private key.

Practice:

It SHOULD be possible to administratively deactivate the key, for example by logging out, turning off the system, or removing the key.

Automatic deactivation of the key SHOULD happen after a certain short duration (order of minutes) of inactivity.

Audit:

□ *Interview: SO.*

□ *Question: How can keys be deactivated?*

□ *Examine: The key storage system.*

□ *Verify: Automatic deactivation occurs after several minutes of inactivity.*

6.3 Activation Data

Activation data is the data required to operate private keys or cryptographic modules containing private keys.

6.3.1 Activation Data Generation and Installation

Objective: Generate secure and trustworthy activation data values.

Control: To generate activation data, use systems that are able to generate unpredictable data values.

Practice:

There are different ways to implement activation data, for example with PINs, passphrases, or key-splitting schemes.

Audit:

□ *Interview: SO.*

□ *Question: What activation data mechanisms are being used?*

□ *Question: Who is responsible for generating the activation data values?*

□ *Question: How is activation data delivered to the authorized personnel?*

6.3.2 Activation Data Protection

Objective: Prevent unwanted exposure and/or modification of private keys.

Control: Implement m-out-of-n controls.

Practice:

Owners of activation data should protect their own credentials. To mitigate against theft of activation data, there SHOULD be at least m persons required to activate the private key, where m > 1. To mitigate against loss of activation data, there should be at least n persons given access to activation data, where n > 2.

Audit:

□ *Interview: SO.*

□ *Question: Are m-out-of-n mechanisms in use for activation data?*

□ *Question: If so, what are the values for m and n?*

6.4 Key Incident Handling

6.4.1 Private Key Compromise

Objective: Allow for a quick recovery after a detected key compromise or loss.

Control: Perform an emergency key rollover.

Practice:

Besides the regular incident response procedures[7], a new key SHOULD be introduced as soon as possible, and the compromised key (and the DS record in case of a KSK) SHOULD be removed

[7] The controls described in section 2.2.2 also applies here.

as soon as the new key and signatures have been propagated to the end client's caches. A new standby SHOULD be published as a DS record in the parent zone.

How and where to request the emergency key rollover SHOULD be known to the entity.

A key can be compromised in different ways:

1. Theft, where the private key materials have been exposed to an attacker.

2. Loss, where the private key materials have become unaccessible.

3. Cryptographic weakness, where the private key materials have become to weak to be secure.

Audit:

□ *Interview: SA.*

□ *Question: What is the procedure for handling a private key compromise?*

□ *Question: Is it known who to contact at the parent zone in case an emergency rollover has to be performed?*

7 Technical Security Controls

Besides key pair handling and computer security controls, there are the concerns of network security. Most of these controls are also listed in RFC 2870 and are not specific to DNSSEC.

7.1 Network Security

This section list the network security related controls, for example firewalls and network topology.

7.1.1 Firewall

Objective: Discourage network access to any port other than those needed for DNS service.

Control: Have different firewall rules for name servers.

Practice:

The LAN segments on which the name servers are homed SHOULD have its own firewall.

7.1.2 Reverse Name Resolution

Objective: Determine the domain name that is associated with the entity's DNS and other services.

Control: Support reverse DNS lookup.

Practice:

The network on which the server is homed SHOULD have in-addr.arpa service.

Audit:

□ *Test: Reverse DNS.*

□ *Validate: Positive responses are being returned for the lookup of PTR records of the entity's name servers.*

7.1.3 Diversity in Network Locations

Objective: Reduce risk of unavailability in case of a network failure.

Control: Name servers are located in separate, unrelated network segments.

Practice:

Secondary name servers SHOULD be located on different network segments.

Audit:

□ *Test: Name server network segments.*

□ *Validate: Name servers are located in different network segments.*

7.1.4 Timestamping

Objective: Keep computer clocks synchronized.

Control: Use clock synchronization tools.

Practice:

The entity SHOULD have their clocks synchronized via NTP or similar mechanisms, in as secure manner as possible. For this purpose, servers and their associated firewalls SHOULD allow the authoritative name servers and signer systems to be NTP clients (but not servers).

To prevent NTP based DoS attacks, the entity MAY use of NTP4 with authentication [18].

Audit:

□ *Interview: SA.*

□ *Question: Are firewalls and servers configured so that name servers can act as NTP client?*

□ *Question: Is NTP4 with authentication used?*

7.2 Life Cycle Technical Controls

This section addresses system development controls and security management controls. No stipulation for the purpose of this audit framework.

8 Zone Signing

This component covers all aspects of zone signing.

8.1 Key Lengths, Key Types and Algorithms

This section focuses on the key parameters, such as their role, key length, and which cryptographic algorithms.

8.1.1 Signing Scheme

Objective: Establish operational flexibility, continuity, and transparency while maintaining trustworthiness in DNS.

Control: Implement a signing scheme.

Practice:

Two signing schemes are possible: A KSK-ZSK Split Signing Scheme or a Single-Type Signing Scheme. The entity SHOULD implement one of these signing schemes based on its operational objectives.

Audit:

- □ *Interview: SO, SA.*
- □ *What are the operational objectives (SLA, access to key material, etc) that made one choose for the existing scheme?*
- □ *Examine: DNSKEY and RRSIG records.*
- □ *Verify: A valid signing scheme is used.*

8.1.2 Cryptographic Parameters

Objective: Signatures can be used to validate integrity and authenticity of DNS resource records.

Control:

Use sufficiently strong key lengths and algorithms for their purpose (DNSSEC validation) and their effective period.

Practice:

Algorithms MUST be standardized by the IETF and SHOULD be chosen such that they comply with a cryptographic standard. RFC 6781 suggests the use of RSA/SHA-256.

Key length SHOULD be based on common security considerations (e.g. NIST's [10]) or a published policy.

Audit:

- □ *Examine: DNSKEY records.*
- □ *Verify: Chosen key lengths and algorithms comply with a cryptographic standard.*
- □ *Verify: Chosen key algorithms are standardized by the IETF.*
- □ *Verify: Chosen key length and the considerations on which it is based.*

8.2 Authenticated Denial of Existence

Authenticated denial of existence is the ability to cryptographically proof that requested resource records do not exist.

8.2.1 NSEC or NSEC3

Objective: Allow for validation of non-existent data.

Control: Implement NSEC or NSEC3.

Practice:

The entity MUST implement either NSEC or NSEC3. NSEC is known to have zone walking issues. NSEC3 solves this not completely, but makes it harder.

If NSEC3 is used, the parameters to use are worth considering. The hash algorithm MUST be SHA-1 (1). The opt-out flag SHOULD be clear, unless there are operational boundaries that (currently) prevent the signing of all delegations. The salt should be at least 64 bits (8 octets) and unpredictable.

Re-salting SHOULD occur periodically and only makes sense in highly dynamic zones. RFC 5155 [19] recommends that the salt is changed every re-signing, but this requires creating (at least) one signature for each signed delegation. Therefor, the re-salting period SHOULD be based on the prediction of the duration of a successful dictionary attack.

Increasing the value of the number of iterations affects the cost of a dictionary attack, but also the signing and validation performance. A NSEC3 Hash Performance research [20] shows that the half performance count for signing is at about 100 iterations, while for validating it varies on the key length and starts at 150 iterations. Therefor, the number of iterations SHOULD be at most set to 100.

Audit:

□ *Interview: SA.*

□ *Question: Is there a rate limiting mechanism to counter zone walking?*

□ *Examine: The signed zone contents.*

□ *Verify: Either NSEC or NSEC3 is implemented.*

□ *Verify: If NSEC3 is implemented, the hash used is SHA-1.*

□ *Verify: If NSEC3 is implemented, opt-out is not used.*

□ *Verify: If NSEC3 is implemented, the salt is at least 8 octets.*

□ *Verify: If NSEC3 is implemented, the iterations are below 100.*

□ *Examine: KASP.*

□ *Verify: Re-salting is implemented in case of NSEC3.*

8.3 Signature Format

Objective: Provide consistency between signatures and key material.

Control: This is implied by the chose key algorithm and signing scheme.

Practice:

The RRSIG records MUST have the same algorithm as the used keys.

The RRsets MUST be signed with the key with the corresponding role (KSK or ZSK).

Audit:

□ *Examine: RRSIG records.*

- □ *Verify: The algorithm corresponds with the algorithm used in the DNSKEY RRset.*
- □ *Verify: The signature over the DNSKEY RRset comes from the KSK.*
- □ *Verify: The signatures over the other RRsets come from the ZSK.*

8.4 Key Rollover

This section describes key rollover controls, that are required to practice operational routine or in conjunction with an incident or a change in policy (for example when a new cryptographic algorithm is required, or when a new key storage is going to be used).

8.4.1 KSK Rollover

Objective: Practice operational routine in order to maintain the chain-of-trust.

Control: Have provisions in place to perform a KSK rollover.

Practice:

A KSK rollover can minimize the number of interactions at the parent (requiring two KSKs in the DNSKEY RRset temporarily), or can choose to publish a standby key (requiring two DS records at the parent) so that the new key can be introduced without any further interactions towards the parent. The first is called Double-Signature Rollover (because of the two required signatures over the DNSKEY RRset), the latter is called a Double-DS Rollover. The entity SHOULD have provisions in place to perform one of those key rollovers.

There are two main school of thoughts on how often a key rollover should occur. First, it should occur periodically, so that the procedure remains an operational routine. Second, it should occur only in conjunction with a change in policy and procedure, or when the key has been compromised. Both arguments are valid.

Audit:

- □ *Interview: SO, SA.*
- □ *Question: What KSK rollover is being used?*
- □ *Question: How often is a KSK rollover performed?*
- □ *Question: Is there a document that describes the KSK rollover procedure?*
- □ *Question: Is it known which third parties rely on the key as a SEP or trust anchor?*
- □ *Question: If the key is used as a trust anchor, is RFC 5011 implemented?*

8.4.2 ZSK Rollover

Objective: Practice operational routine in order to maintain the authenticity and integrity of RRsets.

Control: Have provisions in place to perform a ZSK rollover.

Practice:

The chosen ZSK rollover SHOULD focus on minimizing the number of signatures during the rollover, to keep the DNS response size low. This rollover is commonly referred to as a Pre-publish Key Rollover.

Audit:

- □ *Interview: SO, SA.*
- □ *Question: What ZSK rollover is being used?*
- □ *Question: How often is a ZSK rollover performed?*

□ *Question: Is there a document that describes the ZSK rollover procedure?*

8.4.3 Algorithm Rollover

Objective: Maintain trust in the cryptographic parameters used in DNSSEC.

Control: Have provisions in place to perform an algorithm rollover.

Practice:

When trust in currently used cryptographic parameters weaken, the entity SHOULD be prepared to transition to another standardized algorithm.

Audit:

□ *Interview: SO, SA.*

□ *Question: Is there a document that describes the algorithm rollover procedure?*

8.4.4 Automated Procedure Implementation

Objective: Minimize error in execution of zone signing.

Control: Automate or use scripts to execute the zone signing functions described above.

Practice:

Software or scripts SHOULD be used to perform critical functions that are not operated and not routine, such as key rollovers, zone signing, and other selected aspects of the operation.

The software or scripts SHOULD be able to cope with errors, such as:

□ Delay of publication in the parent zone of the successor DS record.

□ Zone cannot be re-signed due to an occurred incident (e.g. a compromise or disaster).[8]

Said automats and scripts SHOULD be maintained properly.[9]

Audit:

□ *Interview: SA.*

□ *Question: What parts of the zone signing functions are automated, what parts are scripted?*

□ *Question: What type of automation is used?*

□ *Question: What is the maintenance/feedback for improving automation or scripts?*

□ *Review: Scripts or Automation.*

□ *Verify: Existence and level of completeness.*

* Controls for recovery after a compromise or disaster are covered in section 6.4.1.

** Maintenance of these implementations are subject to the controls described in section 5.1.1.

8.5 Signature Lifetime and Re-Signing Frequency

The signature lifetime and re-signing frequency are important controls to provide trustworthy digital signatures.

8.5.1 Re-Signing Frequency

Objective: Provide fresh digital signatures.

[8] Controls for recovery after a key compromise or disaster are covered in section 6.4.

[9] Maintenance of these implementations are subject to the controls described in section 5.1.1.

Control: Re-sign frequently.

Practice:

The re-signing frequency SHOULD be based on the SLA that states how fast updates to the zone are applied. For example, name server operators may promise that a new delegation is live within two hours. In that case, the re-signing frequency SHOULD be higher (twice as high) than the time it takes to process the zone updates, since an update implies a re-sign of the zone. In case of more static zones, the re-signing frequency SHOULD be be in such a way that the refresh period minus the re-sign frequency, minus the maximum signature lifetime jitter sets the time in which operational havoc can be resolved.

A re-sign MUST involve incrementing the SOA SERIAL value.

Audit:

□ *Examine: KASP.*

□ *Verify: The re-signing frequency is either at most twice as high as the zone update frequency, or in case of more static zones, the re-signing frequency is sane with respect to the refresh period and signature lifetime jitter.*

□ *Verify: There is a mechanism that increments the serial as part of a re-sign operation.*

8.5.2 Refresh Period

Objective: Allow for a reasonable long duration to resolve operational havoc without having to worry that signatures will expire.

Control: Refresh signatures long before they expire.

Practice:

Signatures SHOULD be refreshed a sufficient duration before they expire. A sufficient duration depends on the time that the entity's operation may be unmanned or a system may be without power. Suggested duration is a long weekend plus some additional days to resolve the operational havoc, for example 7 days.

Audit:

□ *Examine: KASP and signed zone contents.*

□ *Verify: No signatures expire within the refresh period, minus the re-sign frequency, minus the maximum signature lifetime jitter.*

8.5.3 Signature Lifetime

Objective: Limit exposure when child keys have been compromised.

Control: Limit the risks of replay attacks.

Practice:

To limit the risks of replay attacks, the signature lifetime SHOULD NOT be unnecessary high. The maximum lifetime SHOULD be motivated by standard or specification.

The maximum signature lifetime MUST be higher than the refresh period (specified in the KASP, or by the REFRESH value of the SOA record).

A signature lifetime jitter MAY be applied, to prevent that not all signatures expire at the same time.

Audit:

□ *Interview: SA.*

□ *Question: What is the specified maximum signature validity period?*

□ *Question: What are the motivations for choosing that period.*

□ *Examine: KASP and signed zone contents.*

□ *Verify: All signatures have a shorter validity period than a specified period.*

□ *Verify: All signatures have a longer validity period than the refresh period.*

□ *Verify: A signature lifetime jitter has been applied.*

8.6 Verification of Resource Records

It is good practice to audit the correctness of the signer system.

8.6.1 DNSSEC Checking

Objective: To verify that signatures are valid, DNSKEY is unmodified, and unsigned zone contents are not altered.

Control: Audit the signer system.

Practice:

A tool that audits the signer system SHOULD be used. This tool SHOULD perform the following checks:

□ A heuristic check that gives confidence that signature values of RRSIG records are correctly generated.

□ No RRSIG records are expired.

□ Inception values of RRSIG records are all in the past.

□ Inception and Expiration values of RRSIG comply with the signature validity period as specified by policy. DNSKEY records are correctly published.

□ A heuristic check that gives confidence that the unsigned zone contents have not been altered.

□ A check that validates KSK->ZSK->RRSIG consistency.

Audit:

□ *Examine: The DNSSEC check mechanism.*

□ *Verify: All recommended checks are implemented.*

9 Zone Contents

This section cover all controls related to the contents of the entity's zones.

9.1 Secure Entry Point and Zone Signing Keys

This section describes how to make available the public key material in order to allow stakeholders to validate the integrity and authenticity of the zone's resource records.

9.1.1 In-Band Secure Entry Point Publication

Objective: Allow for building a chain-of-trust towards the particular zone.

Control: Publish public key information in the DNS so that users can build a chain-of-trust to the entity's zone.[10]

[10] This control only partly addresses the objective. The parental registry should also have the same control or the

Practice:

The currently active KSK MUST be published as a DNSKEY in the entity's zone.

The DS corresponding to the currently active KSK SHOULD be published in the parent zone.

Audit:

□ *Examine: The DNSKEY RRset in the entity's zone.*

□ *Verify: The DNSKEY RRset includes the DNSKEY record that corresponds to the current active KSK.*

□ *Examine: The DS RRset of the entity's delegation in the parent zone.*

□ *Verify: The DS RRset contains a DS record that corresponds to the current active KSK.*

□ *Test: Chain-of-trust.*

□ *Validate: A chain-of-trust to the DNSKEY RRset of the entity can be created.*

9.1.2 Standby Secure Entry Point Key

Objective: Allow for a business continuity in case of critical problems with the DNSSEC key material.

Control: Publish a public and maintain a private emergency key[11] to allow for rapid compromise recovery.

Practice:

An in-band publication of the standby key SHOULD be available as a DS record in the parent zone. The standby key MUST be of the same algorithm of the keys in use.

Audit:

□ *Interview: SO.*

□ *Question: Is there a standby SEP key published that enables a rapid emergency key rollover?*

□ *Examine: The DS RRset of the entity as published in the parent zone.*

□ *Verify: The DS RRset contains the DS record that corresponds to the standby key.*

□ *Test: Standby DS Correctness.*

□ *Validate: From the standby public key it is possible to construct the published DS record.*

9.1.3 Link Secure Entry Point to Data Signatures

Objective: Allow for DNSSEC validation for the particular zone.

Control: Publish public key information in the DNS so that users can validate entity's zone.[12]

Practice:

The currently active ZSK MUST be published as a DNSKEY in the entity's zone. This may be the same key as the KSK.

Audit:

control described in section 2.1.2 in place. Assessment of this is out of scope.

[11] Private key controls are discussed in section 6.2.

[12] Controls regarding the signatures are covered in section 8.

□ *Examine: The DNSKEY RRset in the entity's zone.*

□ *Verify: The DNSKEY RRset includes the DNSKEY record that corresponds to the current active ZSK.*

9.1.4 DS Interoperability

Objective: Provide interoperability with chain-of-trust stakeholders, such as validating resolvers.

Control: Publish at least one mandatory DS digest algorithms.

Practice:

At least one DS record MUST be published with one of the algorithms marked as mandatory by IANA [21]. Other digest algorithms may be accepted with additional DS records.

Audit:

□ *Examine: DS records in the entity's zone.*

□ *Verify: Are mandatory DS digest algorithms accepted by the entity.*

□ *Verify: At least one mandatory algorithm per delegation is published.*

9.2 Resource Records Time-to-Live

The Time-to-Live (TTL) of Resource Records determine how long caching resolvers may keep the data in their cache.

9.2.1 Minimum Zone Time-to-Live

Objective: Prevent operational and managerial issues with respect to signature validity periods.

Control: Use a Minimum Zone Time-to-Live (TTL) that is high enough to both fetch and verify all the required Resource Records in the chain-of-trust.

Practice:

RFC 6781 mentions that it has been demonstrated that a TTL under 10 minutes may cause disruptions. Therefor, the Minimum Zone TTL SHOULD be higher than 10 minutes (600 seconds).

Audit:

□ *Examine: Entity's zone TTL.*

□ *Verify: The values are all above 600 seconds.*

9.2.2 Maximum Time-to-Live

Objective: Allow for reasonable quick propagation of zone updates.

Control: Use a Maximum Zone TTL that is a reasonable time for a resolver to store the data in a cache.

Practice:

There exist resolvers that cap the TTL of Resource Records to one day by default. This is considered a reasonable and therefor, the Maximum Zone TTL SHOULD be lower than one day (86400 seconds).

Also, TTL values SHOULD be a fraction of the RRSIG validity period, and lower than the refresh period, so that RRsets expire from resolver caches before its signature expires.

Audit:

□ *Examine: Entity’s zone TTL.*

□ *Verify: The values are all lower than 86400 seconds.*

□ *Verify: The values are a fraction of the RRSIG validity period.*

□ *Verify: The values are lower than the refresh period.*

9.2.3 SOA Expiration Timer

Objective: Make a name server non-authoritative before possible DNSSEC problems become visible.

Control: Use a SOA expiration timers that will allow problems with transfers from the master server to be noticed before signatures time out.

Practice:

RFC 6781 suggests that the SOA expiration timer be approximately one third or a quarter of the minimum signature validity period.

Audit:

□ *Examine: Entity’s minimum signature validity period.*

□ *Verify: The value of the SOA EXPIRE RDATA is at most a third of that signature validity period.*

10 Logging

This section covers all event logging controls.

10.1 Audit Logging Procedures

This section describes controls for event logging, implemented for the purpose of monitoring operations, root-cause analysis in case of an incident, or for statistical purposes.

10.1.1 Type of Logged Events

Objective: Allow for detecting deviating behavior and finding root-causes in case of incident.

Control: Log all relevant access and operations attempts.

Practice:

Entrance attempts to the facility SHOULD be logged (Multi tier access requires logging at each tier).

Remote access attempts to machines that are operationally critical SHOULD be logged.

Privileged operations on these machines SHOULD be logged.

HSM access and operations SHOULD be logged.

Audit:

□ *Interview: SO, SA.*

□ *Question: What type of events are logged?*

□ *Examine: Logs.*

□ *Verify: There are logs that indicate access and usage of the facility, machines and signing systems (e.g. the HSM).*

□ *Test: Facility entrance.*

□ *Verify: The auditor's visit is logged.*

10.1.2 Retention of Logs

Objective: Allow for finding root-causes in case of an incident that has been not immediately discovered.

Control: Archive logs for a certain period.

Practice:

To be able to deal with a late discovered incident, logs SHOULD be archived for at least a year. Such a duration allows for review of incidents during the creation of annual reports.

Audit:

□ *Examine: Logs.*

□ *Verify: The logs go back long enough.*

10.1.3 Protection of Logs

Objective: Provide confidentiality, integrity and availability of the logged events.

Control: Protect logs against loss, manipulation and unauthorized viewing.

Practice:

The logs SHOULD be stored encrypted.

The logs SHOULD be stored at two geographical different locations.

Name server logging SHOULD be to separate hosts which SHOULD be protected similarly to the name servers themselves.

Audit:

□ *Examine: Electronic logs storage.*

□ *Verify: The data is encrypted.*

□ *Verify: There is more than one location where the logs are stored.*

□ *Examine: Paper logs storage.*

□ *Verify: The logs are stored in a safe.*

□ *Verify: The safe is reasonably protected against events like theft or fire.*

10.1.4 Usage of Logs

Objective: Timely detect incidents and other exceptional behavior.

Control: Audit logs.

Practice:

There SHOULD be exception handling mechanisms for logs, so that warnings and errors do not go undetected. Logs MAY be monitored on expected log entries as well.

The actions required in case exceptional or unexpected behavior occurs SHOULD be documented.

Audit:

□ *Interview: SO, SA.*

□ *Question: How are logs being audited?*

□ *Question: Is there an automatic exception detection?*

□ *Question: What actions are triggered in case of the detection of unusual log entries?*

11 Other Controls

This audit framework is subject to revision and extension. The section covers some topics that may also be addressed in a future version of this framework:

- Zone file protection
- Parent policies
- End user policies (resolver compromised, client compromised)
- Active relationships
- Data Corruption
  - Database Corruption
  - Outdated information
  - Modified information
  - System Corruption
  - Resolver compromised
- Protocol Issues
  - Cache Poisoning
  - Open Recursion
  - Additional Section
  - Fragmentation
  - Query Prediction
  - MITM
- Denial of Service
  - System/Application Crash
  - Resource Starvation (defense mechanisms: RRL, Anycast, Ratelimiting)
- Privacy
  - Cache Snooping
  - Zone Enumeration.
- Variation in procedures (procedural errors)
  - By doing variation in involved organizations, you 'automatically' get diversity in hardware, OS, software, network locations, power grids, facility location, procedures, etc.
- Continuity
  - Procedures on how to update and test new software.
- Network
  - No other hosts than the name servers in the LAN.
- Registrar portal

    - Replay attack possibilities?
- Other Concerns
    - Water exposures
    - Off-site backup
    - Operational routine practice

12 Acknowledgement

This document draws heavily on RFC 2870 and 6841. The authors of these documents: Randy Bush, Daniel Karrenberg, Mark Kosters, Raymond Plzak (2870) and Frederik Ljunggren, Anne-Marie Eklund Lowinder, Tomofumi Okubo (6841) are acknowledged for their excellent work.

Special acknowledgments go out to Daniel Stirnimann, Anne-Marie Eklund Lowinder and Scott Rose, who have reviewed this document in an early stage.

NLnet Labs is a not for profit foundation and is subsidized by the NLnet Foundation and SIDN.

This work item was partly funded by a grant from SWITCH, the .CH and .LI registry.

13 License

This document is distributed as PDF. Four a source document in ODT format or any other questions regarding this document please contact the authors:

Matthijs Mekking <matthijs@nlnetlabs.nl>

Olaf Kolkman <olaf@nlnetlabs.nl>

or contact NLnet Labs:

NLnet Labs <info@nlnetlabs.nl>

Bibliography

1: RFC 1034: *DOMAIN NAMES - CONCEPTS AND FACILITIES*, P. Mockapetris, November1987, http://www.rfc-editor.org/rfc/rfc1034.txt

2: RFC 1035: *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*, P. Mockapetris, November1987, http://www.rfc-editor.org/rfc/rfc1035.txt

3: RFC 4033: *DNS Security Introduction and Requirements*, R. Arends, R. Austein, M. Larson, D. Massey, & S. Rose, March2005, http://www.rfc-editor.org/rfc/rfc4033.txt

4: RFC 4034: *Resource Records for the DNS Security Extensions*, R. Arends, R. Austein, M. Larson, D. Massey, & S. Rose, March2005, http://www.rfc-editor.org/rfc/rfc4034.txt

5: RFC 4035: *Protocol Modifications for the DNS Security Extensions*, R. Arends, R. Austein, M. Larson, D. Massey, & S. Rose, March2005, http://www.rfc-editor.org/rfc/rfc4035.txt

6: RFC 2119: *Key words for use in RFCs to Indicate Requirement Levels*, S. Bradner, March1997, http://www.rfc-editor.org/rfc/rfc2119.txt

7: RFC 5730: *Extensible Provisioning Protocol (EPP)*, S. Hollenbeck, August2009, https://www.rfc-editor.org/rfc/rfc5730.txt

8: ISO/IEC, *27002:2005(E): Information technology - Security techniques - Code of practice for information security management* , 2005

9: RFC 6841: *A Framework for DNSSEC Policies and DNSSEC Practice Statements*, F. Ljunggren, AM. Eklund Lowinder & T. Okubo , January2013,

10: R. Chandramouli & S. Rose, *Secure Domain Name System (DNS) Deployment Guide* , September 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

11: RFC 2870: *Root Name Server Operational Requirements*, R. Bush, D. Karrenberg, M. Kosters & R. Plzak, June2000, http://www.rfc-editor.org/rfc/rfc2870.txt

12: RFC 6781: *DNSSEC Operational Practices, Version 2*, O. Kolkman, W. Mekking & R. Gieben, December2012, http://www.rfc-editor.org/rfc/rfc6781.txt

13: ISO/IEC, *ISO27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.* , 2011

14: M. Brooks, The Zombie Survival Guide2003

16: RFC 1305: *Network Time Protocol (Version 3) Specification, Implementation and Analysis*, David L. Mills, March1992, http://www.rfc-editor.org/rfc/rfc1305.txt

17: RFC 4086: *Randomness Requirements for Security*, D. Eastlake, J. Schiller & S. Crocker, June2005, http://www.rfc-editor.org/rfc/rfc4086.txt

18: E. Barker & J. Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* , January 2012 http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

19: RFC 5905: *Network Time Protocol Version 4: Protocol and Algorithms Specification*, D. Mills, J. Martin, Ed., J. Burbank, W. Kasch, June2010, https://www.rfc-editor.org/rfc/rfc5905.txt

20: RFC 5155: *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*, B. Laurie, G. Sisson, R. Arends, D. Blacka , March2008, http://www.rfc-editor.org/rfc/rfc5155.txt

21: Y. Schaeffer, *NSEC3 Hash Performance* , March 2010 http://www.nlnetlabs.nl/downloads/publications/nsec3_hash_performance.pdf

15: IANA Protocol Registry, Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms

14 Appendix I, relation to RFC 6841

RFC 6841 [9] presents a framework to help those who write a DNSSEC Policy Document or a DNSSEC Practice Statement. It provides an extensive list of controls, both technical and non-technical, that should be considered when implementing DNSSEC. In the table below we have replicated the list of topics and provide a mapping to the controls we defined in the framework. The mapping is not one-to-one: The framework has questions that should allow a reviewer to assess whether the 'checklist item' can be ticked or is relevant.

No.	Description	Section Reference
1	Introduction	N.A.
1.1	Overview	N.A.
1.2	Document Name and Identification	N.A.
1.3	Community and Applicability	N.A.
1.4	Specification Administration	N.A.
2	Publication and Repositories	N.A.
2.1	Repositories	2.1 2.2
2.2	Publication of Public Keys	9.1
3	Operational Requirements	N.A.
3.1	Meaning of Domain Names	4.1
3.2	Identification and Authentication of Child Zone Manager	4.2
3.3	Registration of Delegation Signer (DS) Resource Records	4.3
3.4	Method to Prove Possession of Private Key	4.4
3.5	Removal of DS Resource Records	4.5
4	Facility, Management and Operational Controls	N.A.
4.1	Physical Controls	3.1
4.2	Procedural Controls	3.2
4.3	Personnel Controls	3.3
4.4	Audit Logging Procedures	10.1
4.5	Compromise and Disaster Recovery	6.4
4.6	Entity Termination	2.3
5	Technical Security Controls	N.A.
5.1	Key Pair Generation and Installation	6.1
5.2	Private Key Protection and Cryptographic Module Engineering Controls	6.2
5.3	Other Aspects of Key Pair Management	N.A.
5.4	Activation Data	6.3
5.5	Computer Security Controls	5.1
5.6	Network Security Controls	7.1
5.7	Timestamping	7.1.4

5.8	Life Cycle Technical Controls	7.2
6	Zone Signing	N.A.
6.1	Key Lengths, Key Types, and Algorithms	8.1
6.2	Authenticated Denial of Existence	8.2
6.3	Signature Format	8.3
6.4	Key Rollover	8.4
6.5	Signature Lifetime and Re-Signing Frequency	8.5
6.6	Verification of Resource Records	8.6
6.7	Resource Records Time-to-Live	9.2
7	Compliance Audit	N.A.
7.1	Frequency of Entity Compliance Audit	N.A.
7.2	Identify/Qualification of Auditor	N.A.
7.3	Auditor's Relationship to Audited Party	N.A.
7.4	Topics Covered by Audit	N.A.
7.5	Actions Taken as a Result of Deficiency	N.A.
7.6	Communication of Results	N.A.
8	Legal Matters	N.A.

15 Appendix II, relation to NIST-800-81-2

NIST 800-81-2, Secure Domain Name System (DNS) Deployment Guide [10] provides a checklist for deployment of DNSSEC. Again, in the table below we have replicated that checklist and provide a mapping to the controls we defined in the framework. The mapping is not one-to-one: The framework has questions that should allow a reviewer to assess whether the 'checklist item' can be ticked or is relevant.

No.	Description	Section Reference
1	When installing the upgraded version of name server software, the administrator should make necessary changes to configuration parameters to take advantage of new security features.	5.1.1
2	Whether running the latest version or an earlier version, the administrator should be aware of the vulnerabilities, exploits, security fixes, and patches for the version that is in operation in the enterprise. The following actions are recommended: • Subscribe to ISC's mailing list called "bind-announce" or NLnet Labs mailing list "nsd- users" • Periodically refer to the BIND vulnerabilities page at http://www.isc.org/products/BIND/bind-security.html • Refer to CERT®/CC's Vulnerability Notes Database at http://www.kb.cert.org/vuls/ and the NIST NVD metabase at http://nvd.nist.gov/. For other implementations (e.g., MS Windows Server), other announcement lists may exist.	5.1.1
3	To prevent information about which version of server software is running on a system, name servers should be configured to refuse queries for its version.	5.1.1
4	The authoritative name servers for an enterprise should be both network and geographically dispersed. Network-based dispersion consists of ensuring that all name servers are not behind a single router or switch, in a single subnet, or using a single leased line. Geographic dispersion consists of ensuring that not all name servers are in the same physical location, and hosting at least a single secondary server off-site.	3.1.1 7.1.3
5	If a hidden master is used, the hidden authoritative master server should only accept zone transfer requests from the set of secondary zone name servers and refuse all other DNS queries. The IP address of the hidden master should not appear in the name server set in the zone database.	5.2.1
6	For split DNS implementation, there should be a minimum of two physical files or views. One should exclusively provide name resolution for hosts located inside the firewall. It also can contain RRsets for hosts outside the firewall. The other file or view should provide name resolution only for hosts located outside the firewall or in the DMZ, and not for any hosts inside the firewall.	N.A.[13]
7	It is recommended that the administrator create a named list of trusted hosts (or blacklisted hosts) for each of the different types of DNS transactions. In general, the role of the following categories of hosts should be considered for inclusion in the appropriate ACL: • DMZ hosts defined in any of the zones in the enterprise • All secondary name servers allowed to initiate zone transfers • Internal hosts allowed to perform recursive queries.	5.2.1 Some N.A.[14]
8	The TSIG key (secret string) should be a minimum of 112 bits in length if the generator	5.2.1

[13] 'Split View' DNS is considered out of scope for this version.

[14] Some of these checks are not applicable to a public authoritative service

	utility has been proven to generate sufficiently random strings [800-57P1]. 128 bits recommended.	
9	A unique TSIG key should be generated for each set of hosts (i.e. a unique key between a primary name server and every secondary server for authenticating zone transfers). A unique TSIG key should be generated for each set of hosts (i.e. a unique key between a primary name server and every secondary server for authenticating zone transfers).	5.2.1
10	After the key string is copied to the key file in the name server, the two files generated by the dnssec-keygen program should either be made accessible only to the server administrator account (e.g., root in Unix) or, better still, deleted. The paper copy of these files also should be destroyed.	5.2.1
11	The key file should be securely transmitted across the network to name servers that will be communicating with the name server that generated the key.	5.2.1
12	The statement in the configuration file (usually found at /etc/named.conf for BIND running on Unix) that describes a TSIG key (key name (ID), signing algorithm, and key string) should not directly contain the key string. When the key string is found in the configuration file, the risk of key compromise is increased in some environments where there is a need to make the configuration file readable by people other than the zone administrator. Instead, the key string should be defined in a separate key file and referenced through an include directive in the key statement of the configuration file. Every TSIG key should have a separate key file.	5.2.1
13	The key file should be owned by the account under which the name server software is run. The permission bits should be set so that the key file can be read or modified only by the account that runs the name server software.	5.2.1
14	The TSIG key used to sign messages between a pair of servers should be specified in the server statement of both transacting servers to point to each other. This is necessary to ensure that both the request message and the transaction message of a particular transaction are signed and hence secured.	5.2.1
15	Name servers that deploy DNSSEC signed zones or query signed zones should be configured to perform DNSSEC processing.	5.1.3
16	The private keys corresponding to both the ZSK and the KSK should not be kept on the DNSSEC-aware primary authoritative name server when the name server does not support dynamic updates. If dynamic update is supported, the private key corresponding to the ZSK alone should be kept on the name server, with appropriate directory/file-level access control list-based or cryptography-based protections.	6.2.1
17	Signature generation using the KSK should be done offline, using the KSK- private stored offline; then the DNSKEY RRSet, along with its RRSIG RR, can be loaded into the primary authoritative name server.	6.2.1
18	The refresh value in the zone SOA RR should be chosen with the frequency of updates in mind. If the zone is signed, the refresh value should be less than the RRSIG validity period.	5.2.1 8.5.3
19	The retry value in a zone SOA RR should be 1/10th of the refresh value.	5.2.1[15]
20	The expire value in the zone SOA RR should be 2 to 4 weeks.	9.2.3[16]
21	The minimum TTL value should be between 30 minutes and 5 days.	9.2.1[17]
22	A DNS administrator should take care when including HINFO, RP, LOC, or other RR types that could divulge information that would be useful to an attacker, or the external view of a zone if using split DNS. These RR types should be avoided if possible and only used if	N.A.[18]

[15] This framework does not specify a concrete fraction for the retry value.

[16] The expire value is actually a function of the RRSIG validity period.

[17] This framework only recommends a lower bound for the minimum TTL (and it's lower than 30 minutes).

[18] Disclosing information through zone content (other than zone enumeration) is considered out of scope.

	necessary to support operational policy.	
23	A DNS administrator should review the data contained in any TXT RR for possible information leakage before adding it to the zone file.	N.A.[19]
24	The validity period for the RRSIGs covering a zone's DNSKEY RRSet should be in the range of 2 days to 1 week. This value helps reduce the vulnerability period resulting from a key compromise.	8.5.3
25	A zone with delegated children should have a validity period of a few days to 1 week for RRSIGs covering the DS RR for a delegated child. This value helps reduce the child zone's vulnerability period resulting from a KSK compromise and scheduled key rollovers.	8.5.3
26	If the zone is signed using NSEC3 RRs, the salt value should be changed every time the zone is completely resigned. The value of the salt should be random, and the length should be short enough to prevent a FQDN to be too long for the DNS protocol (i.e. under 256 octets).	8.2.1
27	If the zone is signed using NSEC3 RRs, the iterations value should be based on available computing power available to clients and attackers. The value should be reviewed annually and increased if the evaluation conditions change.	8.2.1
28	TTL values for DNS data should be set between 30 minutes (1800 seconds) and 24 hours (86400 seconds).	9.2.2
29	TTL values for RRsets should be set to be a fraction of the DNSSEC signature validity period of the RRSIG that covers the RRset.	9.2.2
30	The (often longer) KSK needs to be rolled over less frequently than the ZSK. The recommended rollover frequency for the KSK is once every 1 to 2 years, whereas the ZSK should be rolled over every 1 to 3 months for operational consistency but may be used longer if necessary for stability or if the key is of the appropriate length. Both keys should have an Approved length according to NIST SP 800-57 Part 1 [800-57P1], [800-57P3].	8.4.1
31	The secure zone that pre-publishes its public key should do so at least one TTL period before the time of the key rollover. [for Zones that pre-publish the new public key]	8.4.2 8.4.4
32	After removing the old public key, the zone should generate a new signature (RRSIG RR), based on the remaining keys (DNSKEY RRs) in the zone file. [for Zones that pre-publish the new public key]	8.4.2 8.4.4
33	A DNS administrator should have the emergency contact information for the immediate parent zone to use when an emergency KSK rollover must be performed.	6.4.1
34	A parent zone must have an emergency contact method made available to its delegated child subzones in case of emergency KSK rollover. There also should be a secure means of obtaining the new KSK.	2.1.1
35	Periodic re-signing should be scheduled before the expiration field of the RRSIG RRs found in the zone. This is to reduce the risk of a signed zone being rendered bogus because of expired signatures.	8.5.1 8.5.2
36	The serial number in the SOA RR must be incremented before re-signing the zone file. If this operation is not done, secondary name servers may not pick up the new signatures because they are refreshed purely on the basis of the SOA serial number mismatch. The consequence is that some security-aware resolvers will be able to verify the signatures (and thus have a secure response) but others cannot.	8.5.1

The checkpoints below all apply to recursive name servers and their use and are out of scope for this framework.

37	Recursive servers/resolvers should be placed behind an organization's firewall and configured to only accept queries from internal hosts (e.g., Stub Resolver host).	N.A.
38	Whenever Aggregate Caches are deployed, the forwarders must be configured to be	N.A.

[19] Disclosing information through zone content (other than zone enumeration) is considered out of scope.

	Validating Resolvers.	
39	Each recursive server must have a root hints file containing the IP address of one or more DNS root servers. The information in the root hints file should be periodically checked for correctness.	N.A.
40	The root hints file should be owned by the account under which the name server software is run. The permission bits should be set so that the root hints file can be read or modified only by the account that runs the name server software.	N.A.
41	Administrators should configure two or more recursive resolvers for each stub resolver on the network.	N.A.
42	Enterprise firewalls should consider restricting outbound DNS traffic from stub resolvers to only the enterprise’s designated recursive resolvers.	N.A.
43	Each recursive server must have a root hints file containing the IP address of one or more DNS root servers. The information in the root hints file should be periodically checked for correctness.	N.A.
44	The root hints file should be owned by the account under which the name server software is run. The permission bits should be set so that the root hints file can be read or modified only by the account that runs the name server software.	N.A.
45	Administrators should configure two or more recursive resolvers for each stub resolver on the network.	N.A.
46	Enterprise firewalls should consider restricting outbound DNS traffic from stub resolvers to only the enterprise’s designated recursive resolvers.	N.A.
47	Non-validating stub resolvers (both DNSSEC-aware and non-DNSSEC- aware) must have a trusted link with a validating recursive resolver.	N.A.
48	Validators should routinely log any validation failures to aid in diagnosing network errors.	N.A.
49	Mobile or nomadic systems should either perform their own validation or have a trusted channel back to a trusted validator.	N.A.
50	Mobile or nomadic systems that perform its own validation should have the same DNSSEC policy and trust anchors as validators on the enterprise network.	N.A.
51	Validator administrator must configure one or more trust anchors for each validator in the enterprise.	N.A.
52	The validator administrator regularly checks each trust anchor to ensure that it is still in use, and updates the trust anchor as necessary.	N.A.