Internet Engineering Task Force (IETF)
Request for Comments: 6841
Category: Informational
ISSN: 2070-1721

F. Ljunggren
Kirei AB
AM. Eklund Lowinder
.SE
T. Okubo
ICANN

January 2013

A Framework for DNSSEC Policies and DNSSEC Practice Statements

Abstract

This document presents a framework to assist writers of DNS Security Extensions (DNSSEC) Policies and DNSSEC Practice Statements, such as domain managers and zone operators on both the top level and secondary level, who are managing and operating a DNS zone with Security Extensions implemented.

In particular, the framework provides a comprehensive list of topics that should be considered for inclusion into a DNSSEC Policy definition and Practice Statement.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6841.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
  1.1. Background 3
  1.2. Purpose 3
  1.3. Scope 4
2. Definitions 4
3. Concepts 6
  3.1. DNSSEC Policy 6
  3.2. DNSSEC Practice Statement 7
  3.3. Relationship between DNSSEC Policy and Practice Statement 7
  3.4. Set of Provisions 9
4. Contents of a Set of Provisions 10
  4.1. Introduction 10
  4.2. Publication and Repositories 11
  4.3. Operational Requirements 12
  4.4. Facility, Management, and Operational Controls 13
  4.5. Technical Security Controls 17
  4.6. Zone Signing 20
  4.7. Compliance Audit 22
  4.8. Legal Matters 23
5. Outline of a Set of Provisions 23
6. Security Considerations 26
7. Acknowledgements 26
8. References 26
  8.1. Normative References 26
  8.2. Informative References 26

1. Introduction

1.1. Background

The Domain Name System (DNS) was not originally designed with strong security mechanisms to provide integrity and authenticity of its data. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system.

The Domain Name System Security Extensions (DNSSEC, [RFC4033], [RFC4034], [RFC4035]) address these vulnerabilities by using public key cryptography to add data origin authentication, data integrity verification, and authenticated denial-of-existence capabilities to the DNS. In short, DNSSEC provides a way for software to verify the origin of DNS data and validate that it has not been modified in transit or by intermediaries.

To provide a means for stakeholders to evaluate the strength and security of the DNSSEC chain of trust, an entity operating a DNSSEC-enabled zone may publish a DNSSEC Practice Statement (DPS), comprising statements describing critical security controls and procedures relevant for scrutinizing the trustworthiness of the system. The DPS may also identify any of the DNSSEC Policies (DPs) it supports, explaining how it meets their requirements.

The DP and DPS are not primarily aimed at users who rely on signed responses from the DNS ("relying parties"); instead, their audience is other stakeholders of the DNS infrastructure, a group that may include bodies such as regulatory authorities.

Even though this document is heavily inspired by the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC3647], with large parts being drawn from that document, the properties and structure of the DNSSEC trust model are fundamentally different from those of the X.509 Public Key Infrastructure (PKI).

1.2. Purpose

The purpose of this document is twofold. Firstly, the document explains the concepts of a DNSSEC Policy (DP) and of a DNSSEC Practice Statement (DPS), and it describes the relationship between the two. Secondly, it presents a framework to encourage and assist writers of Policies and Practice Statements in creating consistent and comparable documents. In particular, the framework identifies the elements that should be considered in formulating a DP or a DPS.

It does not, however, define a particular Policy or Practice Statement, nor does it seek to provide legal advice or recommendations as to the contents.

1.3. Scope

The scope of this document is limited to discussion of the topics that can be covered in a DP or a DPS, but it does not go into the specific details that could possibly be included in either a DP or a DPS. In particular, this document describes the types of information that should be considered for inclusion in them.

This framework should be viewed and used as a checklist of factors that ought be taken into consideration prior to deploying DNSSEC, and as an outline to create an operational practices disclosure document. As such, it focuses on the topics affected by the introduction of DNSSEC into a zone. Other aspects, such as the operations of name servers and registry systems, are considered out of scope. The framework is primarily aimed at Top-Level Domain (TLD) managers and organizations providing registry services, but it may be used by high-value domain holders and so serve as a checklist for DNSSEC readiness at a high level.

This document assumes that the reader is familiar with the general concepts of DNS, DNSSEC, and PKI.

2. Definitions

This document makes use of the following defined terms:

Audit logs: Control evidence information to prove the integrity of processes. This may be generated by DNS and DNSSEC-related systems, supplied by the surrounding facility, or obtained from manually generated, non-electronic documentation. Audit logs will be examined by the internal and/or external auditors.

Activation data: Data values, other than keys, required to operate the cryptographic modules used to protect the keys from unauthorized use.

Chain of trust: A hierarchical structure of trust consisting of DNS keys, signatures, and delegation signer records that, when validated in a series, can provide proof of authenticity of the last element in the chain, providing that the first element is trusted. Usually, the first element is a trust anchor.

Compromise (key compromise): Key compromise is a situation where the private component of a signing key is lost, stolen, exposed, modified, or used in an unauthorized manner. More strictly, even a suspicion that one of these has occurred will be enough to be considered as key compromise.

DNS: The Domain Name System (DNS) is a hierarchical global naming catalog for computers, services, or any resource connected to the Internet.

DNS zone: A portion of the global Domain Name System (DNS) namespace for which administrative responsibility has been delegated.

DNSSEC: DNS Security Extensions (DNSSEC) is a set of IETF specifications [RFC4033] [RFC4034] [RFC4035] that uses public key cryptography to add data origin authentication, data integrity verification, and authenticated denial of existence capabilities to DNS.

DNSSEC Policy: A DNSSEC Policy (DP) sets forth the security requirements and standards to be implemented for a DNSSEC-signed zone.

DNSSEC Practice Statement: A DNSSEC Practice Statement (DPS) is a practices disclosure document that may support and be a supplemental document to the DNSSEC Policy (if such exists), and it states how the management of a given zone implements procedures and controls at a high level.

Key rollover: An operational process to change one of the DNSSEC keys used for signing a zone via distribution of public keys in a trusted manner.

Multi-person control: A security concept to distribute the authority of an operation over multiple persons, to mitigate threats caused by a single authorized individual. For example, a key recovery function may require some number of authorized individuals (m) out of the (n) to whom a portion of the recovery key was distributed, to combine their key fragments, before key recovery can occur.

PKI: Public Key Infrastructure (PKI) is a concept that makes use of asymmetric cryptography to provide a system with integrity, authentication, and confidentiality and to do it via distribution of public keys in a trusted manner.

Policy authority: The body responsible for setting and administering a DNSSEC Policy and for determining whether a DPS is suitable for that Policy.

Relying party: An entity that relies on a signed response from the DNS.

Repository: A location on the Internet to store DP, DPS, trust anchors, and other related information that should be kept public.

Security posture: A security posture is an indicator of how secure an entity is and how secure the entity should be. It is the result of an adequate threat model and risk assessment.

Separation of duties: A security concept that limits the influence of a single person by segregating roles and responsibilities.

Signing key: Private component of an asymmetric key pair that is used for signing of resource records within the zone. Note that the other component, called public key, is used for signature validation.

TLD: A Top-Level Domain (TLD) is one of the domains at the highest level below the root in the hierarchy of the DNS.

Trust anchor: Public portion of a key pair that is the authoritative entity used to authenticate the first element in a chain of trust.

3. Concepts

This section describes the concepts of a DNSSEC Policy and of a DNSSEC Practice Statement. Other related concepts are described as well.

3.1. DNSSEC Policy

A DNSSEC Policy (DP) sets forth requirements that are appropriate for a specified level of assurance. For example, a DP may encompass all topics of this framework, each with a certain set of security requirements, possibly grouped according to impact. The progression from medium to high levels of assurance would correspond to increasing security requirements and corresponding increasing levels of assurance.

A DP also constitutes a basis for an audit, accreditation, or another assessment of an entity. Each entity can be assessed against one or more DPs that it claims to implement.

3.2. DNSSEC Practice Statement

Most zone managers using DNSSEC will not have the need to create a thorough and detailed statement of practices. For example, a registrant may be the sole relying party of its own zone and would already be aware of the nature and trustworthiness of its services. In other cases, a zone manager may provide registration services with only a very low level of assurances where the domain names being secured may pose only marginal risks if compromised. Publishing a DPS is most relevant for entities operating a zone that contains a significant number of delegations to other entities.

A DNSSEC Practice Statement (DPS) should contain information that is relevant to the stakeholders of the relevant zone(s). Since these generally include the Internet community, it should not contain such information that could be considered to be sensitive details of an entity's operations.

A DNSSEC Practice Statement may identify a supported DP, which may subsequently be used by a relying party to evaluate the trustworthiness of any digital signatures verified using the public key of that entity.

3.3. Relationship between DNSSEC Policy and Practice Statement

A DNSSEC Policy and a DNSSEC Practice Statement address the same set of topics of interest to the stakeholders in terms of the level of confidence ascribed to the security posture of a zone. The primary difference is in the focus of their provisions. A Policy sets forth the requirements and standards to be implemented for a DNSSEC-signed zone, and may be used to communicate requirements that must be met by complying parties; as such, it may also be used to determine or establish equivalency between policies associated with different zones. A Practice Statement, by contrast, describes how a zone operator (and possibly other participants in the management of a given zone) implements procedures and controls to meet the requirements of applicable Policies. In other words, the Policy says what needs to be done, and the Practice Statement says what is being done.

An additional difference between a Policy and a Practice Statement relates to the scope of coverage of the two kinds of documents, in terms of its applicability. A Policy may apply to multiple

organizations or multiple zones. By contrast, a Practice Statement would usually apply only to a single zone operator or a single organization, since it describes the actual controls in place that meet the requirements of applicable Policy.

For example, a TLD manager or regulatory authority may define requirements in a Policy for the operation of one or more zones. The Policy will be a broad statement of the general requirements for managing the zone. A zone operator may be required to write its own Practice Statement to support the Policy, explaining how it meets the requirements of the Policy. Alternatively, a zone operator that is also the manager of that zone, and not governed by any external Policy, may still choose to disclose operational practices by publishing a DPS. The zone operator might do so to provide transparency and to gain community trust in its operations.

A Policy and a Practice Statement also differ in the level of detail each expresses: although there may be variations, a Practice Statement will provide a description of procedures and controls and so will usually be more detailed than a Policy, which provides general principles.

The main differences between a Policy and Practice Statement can be summarized as follows:

(a) Operation of a DNS zone with DNSSEC may be governed by a Policy that establishes requirements stating what the entity operating that zone must do. An entity can use a Practice Statement to disclose how it meets the requirements of a Policy or how it has implemented critical processes and controls, absent a controlling Policy.

(b) A Policy may serve the purpose of establishing a common basis of trusted operation throughout a set of zones in the DNS hierarchy. By contrast, a Practice Statement is a statement of a single zone operator or organization.

(c) A Practice Statement is generally more detailed than a Policy and specifies how the zone operator or organization implements critical processes and controls, and how the entity meets any requirements specified in the one or more Policies under which it operates DNSSEC.

3.4. Set of Provisions

A set of provisions is a collection of Policy requirements or Practice Statements, which may employ the approach described in this framework by covering the topics appearing in Section 5 below. The topics are described in detail in Section 4.

A Policy can be expressed as a single set of provisions. A Practice Statement can also be expressed as a single set of provisions with each component addressing the requirements of one or more Policies. Alternatively, it could be a set of provisions that do not reference any particular policy but instead describe a set of self-imposed controls to the stakeholders. For example, a Practice Statement could be expressed as a combination of the following:

(a) a list of Policies supported by the DPS;

(b) for each Policy in (a), a set of provisions that contains statements addressing the requirements by filling in details not stipulated in that policy or expressly left to the discretion of the implementer. Such statements serve to show how this particular Practice Statement implements the requirements of the particular Policy; or

(c) a set of provisions that contains statements regarding the DNSSEC operations practices, independent of any Policy.

The statements provided in (b) may augment or refine the stipulations of an applicable Policy, but generally they must not conflict with the stipulations. In certain cases, however, a Policy authority may permit exceptions because certain compensating controls of the entity disclosed in its Practice Statement allow it to provide a level of assurance equivalent to full compliance with the policy.

The framework outlines the contents of a set of provisions, in terms of eight primary components, as follows:

1. Introduction

2. Publication and Repositories

3. Operational Requirements

4. Facility, Management, and Operational Controls

5. Technical Security Controls

6. Zone Signing

7. Compliance Audit

8. Legal Matters

This framework can be used by Policy authorities to write DNSSEC Policies and by zone operators to write a DNSSEC Practice Statements. Having a set of documents with the same structure facilitates comparisons with the corresponding documents of other zones.

4. Contents of a Set of Provisions

This section describes the contents of a set of provisions. Refer to Section 5 for the complete outline.

Drafters of DPSs conforming to this framework are permitted to add additional levels of subcomponents below those described here to meet specific needs. All components listed in Section 5 should be present, but drafters may leave components empty, only stating "no stipulation", if so required.

4.1. Introduction

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either Policy or Practice Statement) is targeted.

4.1.1. Overview

This subcomponent provides a general introduction to the document. It can also be used to provide a description of entities to which the Policy or Practice Statement applies.

4.1.2. Document Name and Identification

This subcomponent provides any applicable names or other identifiers of the document.

4.1.3. Community and Applicability

This subcomponent identifies the stakeholders along with their expected roles and responsibilities. These include (but are not limited to) an entity signing the zone, entities relying on the signed zone, other entities that have operational dependency on the signed zone, and an entity that entrusted the zone signing.

4.1.4. Specification Administration

This subcomponent contains the contact details of the organization responsible for managing the DP/DPS, as well as the specification change procedures. These procedures may include the description of the notification mechanisms used to provide advance notice of amendments that are deemed to materially affect the assurance provided by the entity and how/when such amendments will be communicated to the stakeholders.

If a Policy authority is responsible for determining whether a DPS is suitable for the Policy, this subcomponent may include the name and contact information of the entity in charge of making such a determination. In this case, the subcomponent also includes the procedures by which this determination is made.

4.2. Publication and Repositories

The component describes the requirements for an entity to publish information regarding its practices, public keys, the current status of such keys together with details relating to the repositories in which the information is held. This may include the responsibilities of publishing the DPS and of identifying documents that are not made publicly available owing to their sensitive nature, e.g., security controls, clearance procedures, or business information.

4.2.1. Repositories

This subcomponent describes the repository mechanisms used for making information available to the stakeholders, and may include:

- The locations of the repositories and the means by which they may be accessed;
- An identification of the entity or entities that operate repositories, such as a zone operator or a TLD manager;
- Access control on published information objects; and
- Any notification services that may be subscribed to by the stakeholders.

4.2.2. Publication of Public Keys

This subcomponent contains information relating to the publication of public keys:

- o Whether the public keys are included in a key hierarchy, published as trust anchors, or both;
- o The data formats and methods available to validate the authenticity of public keys;
- o The frequency and timing of publishing new information (principally, as advance notice for stakeholders relying on the public keys).

4.3. Operational Requirements

This component describes the operational requirements when operating a DNSSEC-signed zone.

4.3.1. Meaning of Domain Names

This subcomponent describes the overall policy of child zone naming, if any.

4.3.2. Identification and Authentication of Child Zone Manager

This subcomponent describes how the child zone manager has initially been identified, and how any subsequent change request is authenticated as originating from the manager or their authorized representative.

4.3.3. Registration of Delegation Signer (DS) Resource Records

This subcomponent describes the process of establishing the chain-of-trust to the child zone by incorporating delegation signer (DS) record(s) into the zone.

4.3.4. Method to Prove Possession of Private Key

This subcomponent describes whether and, if so, under what circumstances the child zone manager is required to provide proof of the possession of the private component of any current or subsequent child zone signing key corresponding to a DS record they wish to incorporate into the parent zone.

4.3.5. Removal of DS Resource Records

This subcomponent will explain how, when, and under what circumstances the DS records may be removed from the zone.

4.4. Facility, Management, and Operational Controls

This component describes non-technical security controls (i.e., physical, procedural, and personnel) in use by the entity to securely perform the DNSSEC related functions. Such controls include physical access, key management, disaster recovery, auditing, and archiving.

These non-technical security controls are critical for trusting the DNSSEC signatures, since lack of security may compromise DNSSEC operations. For example, it could result in the creation of signatures with erroneous information or in the compromise of the signing key.

Within each subcomponent, separate consideration will usually need to be given to each entity type.

4.4.1. Physical Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described. Topics addressed may include:

- Site location and construction, such as requirements for multiple tiers of physical barriers, construction requirements for high-security areas, etc. It may also describe the use of locked rooms, cages, safes, cabinets, etc.;

- Physical access, i.e., mechanisms to control access from one area of the facility to another or additional controls for reaching into higher tiers, such as dual-access control and two-factor authentication;

- Power and air conditioning;

- Water exposures;

- Fire prevention and protection;

- Media storage, e.g., requiring the storage of backup media in a separate location that is physically secure and protected from fire, smoke, particle, and water damage;

- Waste disposal; and

- o Off-site backup.

4.4.2. Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with a description of the responsibilities of each role. Examples of trusted roles include system administrators, security officers, crypto officers, and system auditors.

For each task identified, the number of individuals required to perform the task (m of n rule, if applicable) should be stated for each role. Identification and authentication requirements for each role may also be defined.

This subcomponent also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

4.4.3. Personnel Controls

This subcomponent addresses the following:

- o Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances;

- o Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or other important roles. Such roles may require a check of their criminal records, financial records, references, and any additional clearances required for the position in question;

- o Training requirements and training procedures for each role following the hiring of personnel;

- o Any retraining period and retraining procedures for each role after completion of initial training;

- o Frequency and sequence for job rotation among various roles;

- o Sanctions against personnel for unauthorized actions, such as unauthorized use of authority or unauthorized use of the entity systems;

- o Controls on personnel that are contractors rather than employees of the entity; examples include:

  - * Bonding requirements on contract personnel;

  * Contractual requirements including indemnification for damages due to the actions of the contractor personnel;

  * Auditing and monitoring of contractor personnel; and

  * Other controls on contracting personnel.

- Documentation to be supplied to personnel during initial training, retraining, or otherwise.

4.4.4. Audit Logging Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining an audit trail and to provide evidence of process integrity. Elements include the following:

- Types of events recorded, such as records of key rollover and other key management operations, the personnel assigned to various roles, attempts to access the system, and requests made to the system;

- Frequency with which audit logs are processed or archived, e.g., weekly following an alarm or anomalous event or whenever the audit log size reaches a particular size;

- Period for which audit logs are kept;

- Protection of audit logs:

  * Who can view audit logs, for example, only the audit administrator;

  * Protection against modification of audit logs, for instance, a requirement that no one may modify or delete the audit records or that only an audit administrator may delete an audit file as part of audit file rotation; and

  * Protection against deletion of audit logs.

- Audit log backup procedures;

- Whether the audit log collection function is internal or external to the system;

- Whether the subject who caused an audit event to occur is notified of the audit action; and

- o Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

4.4.5. Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately:

- o Identification or listing of the applicable incident and compromise reporting and handling procedures, which may include the investigation of measures to prevent the event from reoccurring.

- o The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to have been corrupted. These procedures describe how, and under what circumstances, operations of the system are to be suspended; how and when normal operations are resumed; how the stakeholders are to be informed; and how to assess the damage and carry out the root cause analysis.

- o The recovery procedures used if any keys are compromised. These procedures describe how a secure environment is re-established, how the keys are rolled over, how a new trust anchor is provided to the community (if applicable), and how new zone information is published.

- o The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a disaster recovery site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or at a disaster recovery site, for example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

4.4.6. Entity Termination

This subcomponent describes requirements relating to procedures for termination of a contract with an entity, termination notification, and transition of responsibilities to another entity. The purpose may be to ensure that the transition process will be transparent to the stakeholders, and it will not affect the services.

4.5. Technical Security Controls

This component is used to define the security measures taken to protect the cryptographic keys and activation data (e.g., PINs, passwords, or manually held key shares) relevant to DNSSEC operations. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

Also described here are other technical security controls used to perform the functions of key generation, authentication, registration, auditing, and archiving. Technical controls include life cycle security controls, software development environment security, and operational security controls.

If applicable, other technical security controls on repositories, authoritative name servers, or other participants may also be documented here.

4.5.1. Key Pair Generation and Installation

Key pair generation and installation need to be considered, which may involve answering the following questions:

1. Who generates the zone's public/private key pairs? How is the key generation performed? Is the key generation performed by hardware or software?

2. How is the private key installed in all parts of the key management system?

3. How are the zone's public keys provided securely to the parent zone and potential relying parties?

4. Who generates the public key parameters. Is the quality of the parameters checked during key generation?

5. For what purposes may the keys be used, and/or for what purposes should usage of the key be restricted?

4.5.2. Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for key generation and creation of signatures. The following questions may need to be answered:

1. What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the zone's signatures required to be generated using modules compliant with the US FIPS 140-2 [FIPS-140-2] standard? If so, what is the required FIPS 140-2 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests?

2. Is the private key under m of n multi-person control? If yes, provide m and n (two-person control is a special case of m of n, where m = 2 and n >= 2).

3. Is the private key escrowed? If so, who is the escrow agent, in what form is the key escrowed (e.g., plaintext, encrypted, split key), and what are the security controls on the escrow system?

4. Is the private key backed up? If so, who is the backup agent, in what form is the key backed up (e.g., plaintext, encrypted, split key), and what are the security controls on the backup system?

5. Is the private key archived? If so, who is the archival agent, in what form is the key archived (e.g. plaintext, encrypted, split key), and what are the security controls on the archival system?

6. Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (e.g., plaintext, encrypted, or split key)?

7. How is the private key stored in the module (e.g., plaintext, encrypted, or split key)?

8. Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

9. Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.

10. Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and zeroizing the key.

4.5.3. Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the zone operator and other participants. For each of these types of entities, the following questions may need to be answered:

1. What are the life cycle states for the management of any signing keys?

2. What is the operational period of these keys? What are the usage periods or active lifetimes for the pairs?

4.5.4. Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key and potentially needs to be considered for the zone operator and other participants. Such a consideration may need to address the entire life cycle of the activation data from generation through archival and destruction. For each of the entity types, all of the questions listed in Sections 4.5.1 through 4.5.3 potentially need to be answered with respect to activation data rather than with respect to keys.

4.5.5. Computer Security Controls

This subcomponent is used to describe computer security controls such as:

1. use of the trusted computing base concept or equivalent;

2. discretionary access control, labels, mandatory access controls;

3. object reuse;

4. auditing;

5. identification and authentication;

6. trusted path; and

7. security testing.

This subcomponent may also address requirements for product assurance, product evaluation analysis, testing, profiling, product certification, and/or product accreditation.

4.5.6. Network Security Controls

This subcomponent addresses network security related controls, including firewalls, routers, and remote access.

4.5.7. Timestamping

This subcomponent addresses requirements or practices relating to the use of timestamps on various data. It may also discuss whether or not the timestamping application must use a trusted time source.

4.5.8. Life Cycle Technical Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of fail-safe design and implementation techniques (e.g., defensive programming), and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

4.6. Zone Signing

This component covers all aspects of zone signing, including the cryptographic specification surrounding the signing keys, signing scheme, and methodology for key rollover and the actual zone signing. Child zones and other relying parties may depend on the information in this section to understand the expected data in the signed zone

and determine their own behavior. In addition, this section will be used to state the compliance to the cryptographic and operational requirements pertaining to zone signing, if any.

4.6.1. Key Lengths, Key Types, and Algorithms

This subcomponent describes the key generation algorithm, the key types used for signing the key set and zone data, and key lengths used to create the keys. It should also cover how changes to these key lengths, key types, and algorithms may be performed.

4.6.2. Authenticated Denial of Existence

Authenticated denial of existence refers to the usage of NSEC [RFC4034], NSEC3 [RFC5155], or any other mechanism defined in the future that is used to authenticate the denial of existence of resource records. This subcomponent describes what mechanisms are used, any parameters associated with that mechanism, and how these mechanisms and parameters may be changed.

4.6.3. Signature Format

This subcomponent is used to describe the signing method and algorithms used for the zone signing.

4.6.4. Key Rollover

This subcomponent explains the key rollover scheme for each key type.

4.6.5. Signature Lifetime and Re-Signing Frequency

This subcomponent describes the life cycle of the Resource Record Signature (RRSIG) record.

4.6.6. Verification of Resource Records

This subsection addresses the controls around the verification of the resource records in order to validate and authenticate the data to be signed. This may include a separate key set verification process if using a split key signing scheme.

4.6.7. Resource Records Time-to-Live

This subcomponent specifies the resource records' time-to-live (TTL) for all types relevant to DNSSEC, as well as any global parameters that affect the caching mechanisms of the resolvers.

4.7. Compliance Audit

To prove the compliance with a Policy or the statements in the Practice Statement, a compliance audit can be conducted. This component describes how the audit is to be conducted at the zone operator and, possibly, at other involved entities.

4.7.1. Frequency of Entity Compliance Audit

This subcomponent describes the frequency of the compliance audit.

4.7.2. Identity/Qualifications of Auditor

This subcomponent addresses what qualifications are required of the auditor. For instance, it may be that an auditor must belong to a specific association or that they have certain certifications.

4.7.3. Auditor's Relationship to Audited Party

This subcomponent is used to clarify the relationship between the auditor and the entity being audited. This becomes important if there are any requirements or guidelines for the selection of the auditor.

4.7.4. Topics Covered by Audit

Topics covered by audit depends on the scope of the audit. Since the DNSSEC Policy and Practice Statement is the document to be audited against, it is ideal to set the scope of the audit to the scope of the DP/DPS. However, the scope may be narrowed down or expanded as needed, for example, if there are not enough resources to conduct a full audit or if some portion is under development and not ready for the audit.

4.7.5. Actions Taken as a Result of Deficiency

This subcomponent specifies the action taken in order to correct any discrepancy that has a security impact. This could be the remediation process for the audit findings or any other action to correct any discrepancy with the DNSSEC Policy or Practice Statement.

4.7.6. Communication of Results

This subcomponent specifies how the results of the audit are communicated to the stakeholders.

4.8. Legal Matters

The introduction of DNSSEC into a zone may have legal implications. Consequently, it may be appropriate to declare the legal status of the binding embodied in the DNSSEC digital signatures and to clarify on any limitations of liability asserted by the registry manager.

In most cases, the DPS is not a contract or part of a contract; instead, it is laid out so that its terms and conditions are applied to the parties by separate documents, such as registrar or registrant agreements. In other cases, its contents may form part of a legal contract between parties (either directly or via other agreements). In this case, legal expertise should be consulted when drawing up sections of the document that may have contractual implications.

At a minimum, the Legal Matters section should indicate under what jurisdiction the registry is operated and provide references to any associated agreements that are in force. It may also be appropriate to inform of any identified implications on the protection of personally identifiable private information.

5. Outline of a Set of Provisions

This section contains a recommended outline for a set of provisions, intended to serve as a checklist or a standard template for use by DP or DPS writers. Such a common outline will facilitate:

(a) Comparison of a DPS with a DP to ensure that the DPS faithfully implements the policy.

(b) Comparison of two DPSs.

Section 4 of this document is structured so that it provides guidance for each corresponding component and subcomponent of the outline.

```
1.  INTRODUCTION
  1.1.  Overview
  1.2.  Document name and identification
  1.3.  Community and applicability
  1.4.  Specification administration
    1.4.1.  Specification administration organization
    1.4.2.  Contact information
    1.4.3.  Specification change procedures
2.  PUBLICATION AND REPOSITORIES
  2.1.  Repositories
  2.2.  Publication of public keys
3.  OPERATIONAL REQUIREMENTS
  3.1.  Meaning of domain names
```

3.2. Identification and authentication of child zone manager
3.3. Registration of delegation signer (DS) resource records
3.4. Method to prove possession of private key
3.5. Removal of DS resource records
3.5.1. Who can request removal
3.5.2. Procedure for removal request
3.5.3. Emergency removal request
4. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
4.1. Physical controls
4.1.1. Site location and construction
4.1.2. Physical access
4.1.3. Power and air conditioning
4.1.4. Water exposures
4.1.5. Fire prevention and protection
4.1.6. Media storage
4.1.7. Waste disposal
4.1.8. Off-site backup
4.2. Procedural controls
4.2.1. Trusted roles
4.2.2. Number of persons required per task
4.2.3. Identification and authentication for each role
4.2.4. Tasks requiring separation of duties
4.3. Personnel controls
4.3.1. Qualifications, experience, and clearance requirements
4.3.2. Background check procedures
4.3.3. Training requirements
4.3.4. Job rotation frequency and sequence
4.3.5. Sanctions for unauthorized actions
4.3.6. Contracting personnel requirements
4.3.7. Documentation supplied to personnel
4.4. Audit logging procedures
4.4.1. Types of events recorded
4.4.2. Frequency of processing log
4.4.3. Retention period for audit log information
4.4.4. Protection of audit log
4.4.5. Audit log backup procedures
4.4.6. Audit collection system
4.4.7. Vulnerability assessments
4.5. Compromise and disaster recovery
4.5.1. Incident and compromise handling procedures
4.5.2. Corrupted computing resources, software, and/or data
4.5.3. Entity private key compromise procedures
4.5.4. Business continuity and IT disaster recovery capabilities
4.6. Entity termination

5. TECHNICAL SECURITY CONTROLS
5.1. Key pair generation and installation
5.1.1. Key pair generation
5.1.2. Public key delivery
5.1.3. Public key parameters generation and quality checking
5.1.4. Key usage purposes
5.2. Private key protection and cryptographic module engineering controls
5.2.1. Cryptographic module standards and controls
5.2.2. Private key (m-of-n) multi-person control
5.2.3. Private key escrow
5.2.4. Private key backup
5.2.5. Private key storage on cryptographic module
5.2.6. Private key archival
5.2.7. Private key transfer into or from a cryptographic module
5.2.8. Method of activating private key
5.2.9. Method of deactivating private key
5.2.10. Method of destroying private key
5.3. Other aspects of key pair management
5.4. Activation data
5.4.1. Activation data generation and installation
5.4.2. Activation data protection
5.4.3. Other aspects of activation data
5.5. Computer security controls
5.6. Network security controls
5.7. Timestamping
5.8. Life cycle technical controls
6. ZONE SIGNING
6.1. Key lengths, key types, and algorithms
6.2. Authenticated denial of existence
6.3. Signature format
6.4. Key rollover
6.5. Signature lifetime and re-signing frequency
6.6. Verification of resource records
6.7. Resource records time-to-live
7. COMPLIANCE AUDIT
7.1. Frequency of entity compliance audit
7.2. Identity/qualifications of auditor
7.3. Auditor's relationship to audited party
7.4. Topics covered by audit
7.5. Actions taken as a result of deficiency
7.6. Communication of results
8. LEGAL MATTERS

6. Security Considerations

The sensitivity of the information protected by DNSSEC at different tiers in the DNS tree varies significantly. In addition, there are no restrictions as to what types of information (i.e., DNS records) that can be protected using DNSSEC. Each relying party must evaluate its own environment and the chain of trust originating from a trust anchor, the associated threats and vulnerabilities, to determine the level of risk it is willing to accept when relying on DNSSEC-protected objects.

7. Acknowledgements

This document is inspired by RFC 3647 and its predecessor (RFC 2527), and the authors acknowledge the work in the development of these documents.

In addition, the authors would like to acknowledge the contributions made by Richard Lamb, Jakob Schlyter, and Stephen Morris.

8. References

8.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

8.2. Informative References

[FIPS-140-2] NIST, "Security Requirements for Cryptographic Modules", June 2005, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

Authors' Addresses

Fredrik Ljunggren
Kirei AB
P.O. Box 53204
Goteborg SE-400 16
Sweden

EMail: fredrik@kirei.se

Anne-Marie Eklund Lowinder
.SE (The Internet Infrastructure Foundation)
P.O. Box 7399
Stockholm SE-103 91
Sweden

EMail: amel@iis.se

Tomofumi Okubo
Internet Corporation For Assigned Names and Numbers
4676 Admiralty Way, Suite 330
Marina del Ray, CA 90292
USA

EMail: tomofumi.okubo@icann.org