Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 13, 2011

F. Ljunggren
Kirei AB
A-M. Eklund-Lowinder
.SE
T. Okubo
ICANN
November 9, 2010

DNSSEC Policy & Practice Statement Framework
draft-ietf-dnsop-dnssec-dps-framework-03

Abstract

This document presents a framework to assist writers of DNSSEC Policy and Practice Statements such as Domain Managers and Zone Operators on both the top-level and secondary level, who is managing and operating a DNS zone with Security Extensions (DNSSEC) 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 Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 13, 2011.

Copyright Notice

Copyright (c) 2010 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 4
1.1. Background 4
1.2. Purpose 5
1.3. Scope 5
2. Definitions 5
3. Concepts 7
3.1. DP 7
3.2. DPS 7
3.3. Relationship between DNSSEC Policy and Practice Statement 8
3.4. Set of Provisions 9
4. Contents of a set of provisions 10
4.1. Introduction 10
4.1.1. Overview 10
4.1.2. Document Name and Identification 11
4.1.3. Community and Applicability 11
4.1.4. Specification Administration 11
4.2. Publication and Repositories 11
4.3. Operational Requirements 12
4.3.1. Meaning of domain names 12
4.3.2. Activation of DNSSEC for child zone 12
4.3.3. Identification and authentication of child zone manager 12
4.3.4. Registration of delegation signer (DS) resource records 12
4.3.5. Method to prove possession of private key 12
4.3.6. Removal of DS resource records 12
4.4. Facility, Management and Operational Controls 12
4.4.1. Physical Controls 13
4.4.2. Procedural Controls 13
4.4.3. Personnel Controls 14
4.4.4. Audit Logging Procedures 14
4.4.5. Compromise and Disaster Recovery 15
4.4.6. Entity termination 16
4.5. Technical Security Controls 16
4.5.1. Key Pair Generation and Installation 16
4.5.2. Private Key Protection and Cryptographic Module Engineering Controls 17

4.5.3. Other Aspects of Key Pair Management 18
4.5.4. Activation data 18
4.5.5. Computer Security Controls 18
4.5.6. Network Security Controls 19
4.5.7. Timestamping 19
4.5.8. Life Cycle Technical Controls 19
4.6. Zone Signing 20
4.6.1. Key lengths and algorithms 20
4.6.2. Authenticated denial of existence 20
4.6.3. Signature format 20
4.6.4. Zone Signing Key Roll-Over 20
4.6.5. Key Signing Key Roll-Over 20
4.6.6. Signature life-time and re-signing frequency 20
4.6.7. Verification of Zone Signing Key Set 20
4.6.8. Verification of resource records 21
4.6.9. Resource records time-to-live 21
4.7. Compliance Audit 21
4.7.1. Frequency of entity compliance audit 21
4.7.2. Identity/qualifications of auditor 21
4.7.3. Auditor's relationship to audited party 21
4.7.4. Topics covered by audit 21
4.7.5. Actions taken as a result of deficiency 22
4.7.6. Communication of results 22
4.8. Legal Matters 22
4.8.1. Fees 22
4.8.2. Financial responsibility 22
4.8.3. Confidentiality of business information 23
4.8.4. Privacy of personal information 23
4.8.5. Limitations of liability 23
4.8.6. Term and termination 23
5. Outline of a set of provisions 24
6. Security Considerations 27
7. Acknowledgements 27
8. References 27
8.1. Normative References 27
8.2. Informative References 28
Authors' Addresses 28

1. Introduction

1.1. Background

The DNS was not originally designed with strong security mechanisms to provide integrity and authenticity of DNS 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]) is a set of IETF specifications which addresses these vulnerabilities by adding data origin authentication, data integrity verification and authenticated denial of existence capabilities to the Domain Name System, using public key cryptography. In short, DNSSEC provides a way for software to validate that Domain Name System (DNS) data has not been modified during transit.

To provide means for the relying parties to evaluate the strength and security of the DNSSEC chain of trust, an entity operating a DNSSEC enabled zone may choose to publish a DNSSEC Practice Statement (DPS), comprising statements of critical security controls and procedures relevant for scrutinizing the trustworthiness of the system. The DPS may also identify one or more DNSSEC Policies which are supported, explaining how it meets the requirements of each Policy.

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

In the DNSSEC PKI there is no central control of assurance or trust levels. Each zone manager may select their own way of managing keys and operations, and there is no necessity to perform any coordination of security practices between different zones in the DNS. The degree to which a relying party can trust the binding embodied in the DNSSEC chain of trust is dependent on the weakest link of that chain. This implies that the security of zones is generally more critical higher up in the DNS hierarchy.

Another significant difference is that the DPS is focused only on stating the security posture of a zone, and not the entire domain name system. Moreover, the DNS is of a almost ubiquitous nature and completely open. There exists no agreements with the relying (third) parties, which is all entities relying on signed responses from the DNS.

1.2. Purpose

The purpose of this document is twofold. Firstly, the document aims to explain the concept of a DNSSEC Policy (DP) and a DNSSEC Practice Statement (DPS), and describe the relationship between a DP and a DPS. Second, this document aims to present a framework to encourage and assist writers of Policies and Practice Statements in creating heterogenous and comparable documents. In particular, the framework identifies the elements that should be considered in formulating a DP/DPS. It does not, however, define a particular Policy or Practice Statement, not 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/DPS and does not go into the specific details that could possibly be included in each one. In particular, this document describes the types of information that should be considered for inclusion in a DP/DPS.

The DNSSEC Policy and Practice Statement framework should be viewed and used as a checklist of factors that should be taken in to consideration prior to deploying DNSSEC, and an outline to create a operational practices disclosure document. It is primarily aimed at TLD managers and organizations providing registry services, but may be used by high-value domain holders and serve as a check sheet 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 generated by DNS and DNSSEC-related systems, the surrounding facility or other manually processed, non-electronic documentation to prove the integrity of processes. Audit logs will be examined by the internal and/or external auditors.

Activation data - Data values, other than keys, that are required to operate the cryptographic modules which are usually 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 using the first element in the chain. Usually, the first element is a trust anchor.

Compromise (Key Compromise) - Key Compromise is a situation where the private component of the Key Signing Key or Zone 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. It associates various information with domain names assigned to each of the participants.

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

DNSSEC Policy - A DNSSEC Policy sets forth the requirements and standards to be implemented for a DNSSEC signed zone. A Practice Statement may support a Policy by explaining how it meets the requirements of the Policy.

DNSSEC Practice Statement - A DNSSEC Practices Statement is a practices disclosure document which may be a supplemental document to the DNSSEC Policy (if such exists) and states how the management of a given zone implements procedures and controls at a high level.

Key Roll Over - A operational process of DNSSEC to change either the Key Signing Key or the Zone Signing Key.

Policy Management Authority - A group formed by stake-holders from each group within the organization operating DNSSEC, responsible for managing the DP/DPS.

Public Key Infrastructure - A concept that uses asymmetric cryptography, which may provide integrity, authentication, confidentiality and non-repudiation to a system.

Relying Party - An entity that rely on the 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 a barometer that indicates how secure the entity is and how secure the entity should be which is

a result of an adequate threat modelling, vulnerability assessment and risk assessment.

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

Trust Anchor - Public portion of the Key Signing Key which is the authoritative entity used to cryptographically validate the chain of trust to the signed resource record.

3. Concepts

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

3.1. DP

The DP sets forth requirements that are appropriate for a determined level of assurance. For example, a DP may encompass all topics of this framework, each with a certain set of security requirements and possibly grouped them into categories, such as medium impact and high impact. The progression from medium to high levels would correspond to increasing security requirements and corresponding increasing levels of assurance.

A DPS 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.

DPs also constitute a basis for an audit, accreditation, or another assessment of an entity. Each entity can be assessed against one or more DPs that it is recognized as implementing.

3.2. DPS

Most DNSSEC participants may not have the need to create a thorough and detailed statement of practices. For example, the registrant may itself 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 providing 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 which contains a significant number of delegations to other entities.

A DPS should contain information which is relevant to the stakeholders of the relevant zone(s). Since these generally include

the Internet community, it should not contain such information which could be considered to be sensitive details of an entity's operations.

3.3. Relationship between DNSSEC Policy and Practice Statement

A DNSSEC Policy and a DNSSEC Practice Statement address the same set of topics that are of interest to the stakeholders in terms of the degree to which a DNSSEC digital signature may be trusted. Their 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. In other words, the purpose of the Policy is to establish what entities must do. A Practice Statement, by contrast, states how a zone operator (and possibly other participants in the management of a given zone) implements procedures and controls to meet the requirements stated in the Policy. To summarise, the purpose of the Practice Statement is to disclose how the participants perform their functions and implement controls.

An additional difference between a Policy and a Practice Statement relates the scope of coverage of the two kinds of documents. Since a Policy is a statement of requirements, it is best used for communicating minimum operating guidelines that must be met by complying parties, but may as such also be used to facilitate interoperation of a level of trust between zones. Thus, 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.

For example, a TLD Manager or regulatory authority may define requirements in a Policy for operations 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 by explaining how it meets the requirements of the Policy. Or, a zone operator which 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, for the purpose of providing transparency and gain community trust in the operations.

A Policy and a Practice Statement also differ in the level of detail of the provisions in each. Although the level of detail may vary, a Practice Statement will generally be more detailed than a Policy. A Practice Statement provides a detailed description of procedures and controls in place to meet the Policy requirements, while a Policy is more general.

The main differences between a Policy and Practice Statement can

therefore be summarized as follows:

(a) Operation of a DNS zone with DNSSEC may be governed by a Policy, to establish requirements that state 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.
(b) A Policy may facilitate interoperation of level of trust through several parts or levels 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. They are also described in detail in Section 4 below.

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 provisions to the relying parties. 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 responding to that Policy by filling in details not stipulated in that policy or expressly left to the discretion of the implementor; 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 practices of the DNSSEC operations, regardless of any Policy.

The statements provided in (b) may augment or refine the stipulations of an applicable Policy, but generally must not conflict with any of the stipulations of such Policy. In certain cases, however, a Policy Authority may permit exceptions because certain compensating controls

of the entity are disclosed in its Practices Statement, that allow the entity to provide assurances that are equivalent to the assurances provided by entities that are in full compliance with the Policy.

This 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 zone operators to write a DNSSEC Practice Statements. Having a set of documents with the same structure facilitates comparisons and mappings between them 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 in conformance with this framework are permitted to add additional levels of subcomponents below the subcomponents described here for the purpose of meeting the needs of the drafter's particular requirements. Drafters may also leave any components without stipulation if so requires, but all components listed in Section 5 should exist.

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 the Policy or the Practice Statement) is targeted.

4.1.1. Overview

This subcomponent provides a general introduction to the document being written. 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 addresses the stakeholders in DNSSEC along with the expected roles and responsibilities. These include (but are not limited to) an entity signing the zone, an entity that relies 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 includes the name and contact details of the organization that is responsible for managing the DP/DPS.

Moreover, if a formal or informal Policy Authority is responsible for determining whether a DPS being suitable for the Policy this subcomponent may include the name and contact information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

4.2. Publication and Repositories

This component contains any applicable provisions regarding:

- The location and method to access the repository;
- An identification of the entity or entities that operate repositories within the community, such as a zone operator or a TLD Manager;
- The responsibility of an entity to publish information regarding its practices, public keys, and the current status of such keys, which may include the responsibilities of making the DPS publicly available using various mechanisms and of identifying components and subcomponents. It should also include an indication of the elements of the documents that are not made publicly available owing to their sensitive nature, e.g. security controls, clearance procedures, or business information;
- When information must be published and the frequency of publication; and
- Access control on published information objects.

4.3. Operational Requirements

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

4.3.1. Meaning of domain names

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

4.3.2. Activation of DNSSEC for child zone

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

4.3.3. Identification and authentication of child zone manager

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

4.3.4. Registration of delegation signer (DS) resource records

This section describes how the delegation signer resource records are incorporated into the parent zone.

4.3.5. Method to prove possession of private key

This section describes how, if, or under which circumstances the child zone manager is required to provide proof of the possession of the private component of any current or subsequent child zone Key Signing Key that corresponds to a DS record they whish to incorporate into the parent zone.

4.3.6. Removal of DS resource records

This section will explain how, when and under which 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 controls) in use by the entity to securely perform the DNSSEC related functions such as physical access, key management, disaster recovery, auditing and archiving.

These non-technical security controls are critical for trusting the signatures since lack of security may compromise DNSSEC operations

resulting for example, in the creation of signatures with erroneous information or compromising the Key Signing Key and/or Zone Signing Key.

Within each subcomponent, separate consideration will, in general, 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 the construction requirements for high-security areas and the use of locked rooms, cages, safes, and cabinets;
- Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating DNSSEC operations in a secure computer room monitored by guards, cameras or security alarms and requiring movement from zone to zone to be accomplished using tokens and/or PINs;
- Power and air conditioning;
- Water exposures;
- Fire prevention and protection;
- Media storage, for example, 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
- Off-site backup.

4.4.2. Procedural Controls

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

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

This component 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:

- 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 that candidates for these positions must have before being hired;
- Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or perhaps other important roles; such roles may require a check of their criminal records, financial records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;
- Training requirements and training procedures for each role following the hiring of personnel;
- Any retraining period and retraining procedures for each role after completion of initial training;
- Frequency and sequence for job rotation among various roles;
- Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of the entity systems;
- Controls on personnel that are independent 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 provide evidence of processes' integrity. Elements include the following:

- Types of events recorded, such as attempts to access the system, and requests made to the system;
- Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or when ever the audit log is n% full;

- 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 rotating the audit file; and
  - Protection against deletion of audit logs.
- Audit log back up 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
- 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:

- Identification or listing of the applicable incident and compromise reporting and handling procedures.
- The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is re-established, whether the Key Signing Key or Zone Signing key requires a roll over, how to assess the damage and carry out the root cause analysis.
- The recovery procedures used if the Key Signing Key or Zone Signing Key is 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 users (if applicable) and how new zone is published.
- 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 entity termination, termination notification and transition of responsibilities of a zone operator or other entity, where the purpose may be to ensure that the transition process will be transparent to the relying parties and 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 the 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 describes 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 (including 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, whereas the following questions potentially need to be answered:

1. Who generates the zone's public, private key pairs? Furthermore, 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 zones's public keys provided securely to the parent zone and potential relying parties?
4. Who generates the public key parameters, and 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 potentially 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 zones signatures required to be generated using modules compliant with the US 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 n out of m multi-person control? If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?
3. Is the private key escrowed? If so, who is the escrow agent, what form is the key escrowed in (examples include 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, what form is the key backed up in (examples include 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, what form is the key archived in (examples include 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 (i.e., plaintext, encrypted, or split key)?
7. How is the private key stored in the module (i.e., 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. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system?
2. What is the operational period of the 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 consideration potentially needs 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 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 re-use;
4. auditing;
5. identification and authentication;
6. trusted path; and
7. security testing.

Product assurance may also be addressed.

A computer security rating for computer systems may be specified. The rating could be based, for example, on a protection profile (PP) of the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent may also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

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 time-stamping 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 failsafe 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 Key Signing Key and Zone Signing Key, signing scheme and methodology for key roll-over 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 and algorithms

This subcomponent describes the key generation algorithm and the key length used to create the Key Signing Key and the Zone Signing Key.

4.6.2. Authenticated denial of existence

Authenticated denial of existence refers to the usage of NSEC (RFC 4034 [RFC4034]), NSEC3 (RFC 5155 [RFC5155]) or any other record defined in the future that is used to authenticate the denial of existence of the resource record.

4.6.3. Signature format

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

4.6.4. Zone Signing Key Roll-Over

This subcomponent explains the Zone signing key roll-over scheme.

4.6.5. Key Signing Key Roll-Over

This subcomponent addresses the Key signing key roll-over scheme.

4.6.6. Signature life-time and re-signing frequency

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

4.6.7. Verification of Zone Signing Key Set

This subsection addresses the controls around the keyset signing process performed by the Key Signing Key. The procedures surrounding KSK management may be different from those of the ZSK, hence it may be necessary to authenticate the data signed by the KSK.

4.6.8. 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.

4.6.9. Resource records time-to-live

This subcomponent specifies the time-to-live (TTL) for each DNSSEC related resource record such as DNSKEY, NSEC/NSEC3, DS and RRSIG.

4.7. Compliance Audit

The ideal and the only way to prove the compliance with a Policy or the statements in the Practices Statement is to conduct an audit. This component describes the outline of how the audit is 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 is the qualifications for the auditor. For instance it may be an auditor from a specific association or an auditor that has a 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 refers to the scope of the audit. Since the DNSSEC Policy and Practices Statement is the document to be audited against, it is ideal to set the scope to the scope of the DP/DPS. However, the scope may be narrowed down or expanded as needed for example in case there are not enough resources to conduct a full audit, or 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. This could be the remediation process for the audit findings or any other action to correct any discrepancy with the DNSSEC Policy or Practices 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

This component covers legal matters. Sections 8.1 and 8.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations. The remaining sections are generally concerned with legal topics.

With respect to many of the legal subcomponents within this component, a DPS drafter may choose to include in the document terms and conditions that apply directly to registrants or relying parties. For instance, a Registry Manager may set forth limitations of liability that apply to registrants and relying parties. The inclusion of terms and conditions is likely to be appropriate only where the DPS is itself a contract or part of a contract.

In most cases, however, 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, which may include associated agreements, such as registrar or registrant agreements. In that event, a drafter may write a Policy so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements.

4.8.1. Fees

This subcomponent contains any applicable provisions regarding fees charged for DNSSEC or services related to DNSSEC.

4.8.2. Financial responsibility

This subcomponent contains requirements or disclosures relating to the resources available to the zone operator, and to remain solvent if they are liable to pay a judgment or settlement in connection with a claim arising out of such operations.

4.8.3. Confidentiality of business information

This subcomponent contains provisions relating to the treatment of confidential business information. Specifically, this subcomponent addresses:

- The scope of what is considered confidential information;
- The types of information that are considered to be outside the scope of confidential information; and
- The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

4.8.4. Privacy of personal information

This subcomponent relates to the protection that participants, particularly a Registry Operator, may be required to afford to personally identifiable private information of registrants and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law:

- The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy;
- Information that is or is not considered private;
- Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties;
- Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information; and
- Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

4.8.5. Limitations of liability

This subcomponent can include limitations of liability in a DPS or limitations that appear or must appear in an agreement associated with the DPS, such as a registrar or registrant agreement.

4.8.6. Term and termination

This subcomponent can include the time period in which a DPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be

terminated. In addition or alternatively, the DP may include requirements that certain term and termination clauses appear in agreements, such as registrar or registrant agreements. In particular, such terms can include:

- The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.
- Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.
- Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

5. Outline of a set of provisions

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 key signing keys
   - 2.3. Access controls on repositories
3. OPERATIONAL REQUIREMENTS
   - 3.1. Meaning of domain names
   - 3.2. Activation of DNSSEC for child zone
   - 3.3. Identification and authentication of child zone manager
   - 3.4. Registration of delegation signer (DS) resource records
   - 3.5. Method to prove possession of private key
   - 3.6. Removal of DS record
     - 3.6.1. Who can request removal
     - 3.6.2. Procedure for removal request
     - 3.6.3. 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. Retraining frequency and requirements
4.3.5. Job rotation frequency and sequence
4.3.6. Sanctions for unauthorized actions
4.3.7. Contracting personnel requirements
4.3.8. 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. Notification to event-causing subject
4.4.8. 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
5.3.1. Public key archival
5.3.2. Key usage periods
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
5.8.1. System development controls
5.8.2. Security management controls
5.8.3. Life cycle security controls
6. ZONE SIGNING
6.1. Key lengths and algorithms
6.2. Authenticated denial of existence
6.3. Signature format
6.4. Zone signing key roll-over
6.5. Key signing key roll-over
6.6. Signature life-time and re-signing frequency
6.7. Verification of zone signing key set
6.8. Verification of resource records
6.9. 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
8.1. Fees
8.2. Financial responsibility
8.3. Confidentiality of business information
8.3.1. Scope of confidential information
8.3.2. Information not within the scope of confidential

information
8.3.3. Responsibility to protect confidential information
8.4. Privacy of personal information
8.4.1. Information treated as private
8.4.2. Information not deemed private
8.4.3. Responsibility to protect private information
8.4.4. Disclosure Pursuant to Judicial or Administrative Process
8.5. Limitations of liability
8.6. Term and termination
8.6.1. Term
8.6.2. Termination
8.6.3. Dispute resolution provisions
8.6.4. Governing law

6. Security Considerations

The sensitivity of the information protected by DNSSEC on all levels in the DNS tree will vary significantly. In addition, there are no restrictions as to what types of information that can be protected using DNSSEC. Entities must evaluate their own environment and the chain of trust originating from their Trust Anchor, the associated threats and vulnerabilities, to determine the level of risk they are willing to accept.

7. Acknowledgements

The authors gratefully acknowledges, in no particular order, the contributions of the following persons:
Richard Lamb
Jakob Schlyter
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

[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