.se

Recommendations for DNSSEC deployment at municipal administrations and similar organisations

kirei

Recommendations for DNSSEC deployment at municipal administrations and similar organisations

Contents

1 Introduction

1.1 Background

In 2012, the Regional Council in Kalmar County conducted a project with the aim of deploying DNSSEC in the region's municipal administration. The project was carried out with the support of the County Administrative Board in Kalmar County in collaboration with the Swedish Civil Contingencies Agency (MSB) and resulted in all municipal administration in Kalmar county utilizing the DNSSEC security mechanisms.

During the project, the Regional Council in Kalmar County documented experiences and approaches in a guide to support the work of the municipalities. This guide is based on the guide produced by the Regional Council in Kalmar County, but is also, in some sections, reworked to suit a wider target group.

The manuscript for the guide was written by Fredrik Ljunggren and Jakob Schlyter, Kirei AB, and edited by Anne-Marie Eklund Löwinder, .SE. Comments on the content have been obtained from the MSB, the Swedish Post and Telecom Authority (PTS), the Swedish Association of Local Authorities and Regions (SALAR), as well as from .SE's DNS reference group. Editing och publication of this guide has been funded by .SE.

1.2 Goal

In principle, all Internet services depend on the domain name system (DNS). The consequences of any error in the zone data can be extensive. This applies at an increasingly higher degree after the deployment of DNSSEC in a zone. DNSSEC is a cryptographic method for adding data origin authentication and data integrity verification to the zone data, which sets more stringent requirements for operational and technical control than standard DNS.

This guide has been prepared to serve as an aid and a tool for municipalities that are in the process of deploying DNSSEC. The ambition is that it will also provide support for ongoing DNSSEC operations. Naturally, the guide will also function for other types of organisations in both public and private sector.

1.3 Funding

Together with .SE, SALAR and the PTS, the MSB has enabled municipalities in Sweden to obtain funding for the deployment of DNSSEC through the county administrative boards.

For each fiscal year, the MSB has the ability to provide funds from the so-called Appropriation bill 2:4 Crisis Contingencies, that can be applied for by the official agencies indicated. Starting in 2012, the MSB prioritized measures to increase robustness and to facilitate secure online

address resolving using the DNS. Among other actions, the agency has stressed the urgency that domains for public websites to be signed with DNSSEC. The same message is promoted by the highest political leadership, the Minister for Information Technology Anna-Karin Hatt, in the Digital Agenda for Sweden.

1.4 Structure

The guide is divided into three chapters and two appendices (see figure 1.1):

- The chapter *Requirements* is intended to be used as a recommendation and checklist when stating requirements for procurements and system design. The recommendations are divided into a number of categories depending on which parts of a DNS implementation they apply to.
- The chapter *Recommendations for Technical Parameters* is intended to be used as the basis for configuration of a complete system.
- The chapter *Operation and Management* covers a number of areas that are impacted by the deployment of DNSSEC.
- *Appendix A* formulates a governing policy for DNSSEC based on the recommendations set out in this guide.
- *Appendix B* comprises an example of technical controls in compliance with the guide's recommendations.

The notation *Rx*, where R means requirement, is used for requirements that should be considered when deploying DNSSEC.

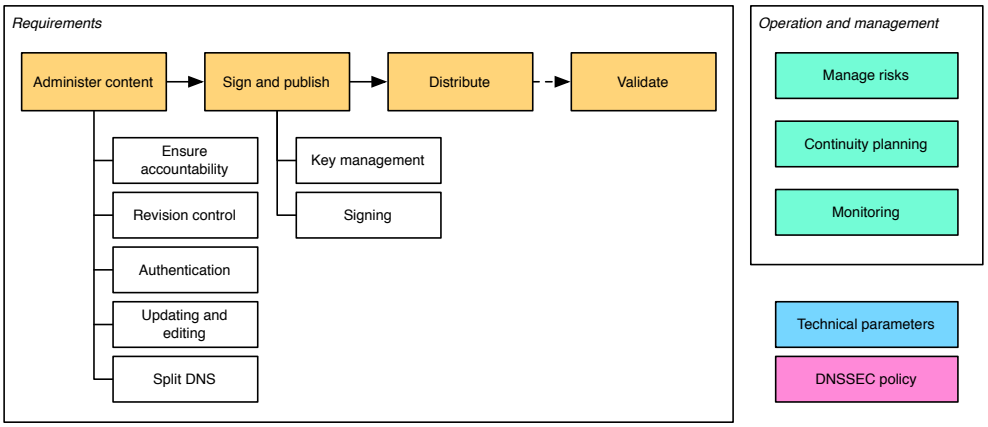


Figure 1.1 – Document structure

1.5 More on the DNS and DNSSEC

The Domain Name System (DNS)[9] is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It

associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

A domain name[10] (for instance, “example.com”) is an identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

Domain names are used in various networking contexts and application-specific naming and addressing purposes. In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server hosting a web site, or the web site itself or any other service communicated via the Internet.

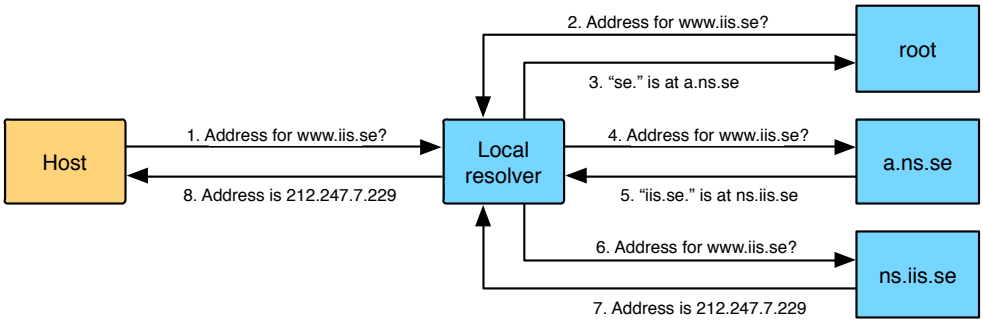


Figure 1.2 – Delegation

When DNS was originally designed in the 1980s, the main idea was to minimize central administration of the network and make it easy to connect new computers to the Internet. There was, however, not much emphasis on security. The deficiencies in this area have opened for various types of abuse and attacks where the responses to DNS lookups are falsified. In this manner, Internet users can be misguided; e.g., people can be tricked into disclosing sensitive information such as passwords and credit card numbers.

Even though every effort has been made to patch security holes in the software tools used for DNS lookups, the fundamental problem lies within the functioning of DNS itself. For this reason, DNSSEC (DNS Security Extensions) have been developed. With DNSSEC, the DNS is secured from abuse by introducing electronic signatures into the DNS data. This ensures that the responses can be validated to be originating from the right source and to have not been manipulated during transmission.

.SE has prepared a brief description of DNSSEC and what DNSSEC protects against. The description is available for download at:
`https://www.iis.se/english/domains/tech/dnssec/`.

2 Requirements

This chapter contains recommended requirements for organisations such as municipal administrations deploying DNSSEC. These recommendations are based on best practices for DNSSEC operations in mission-critical secondary-level domains. Naturally, these recommendations may require adaptation to better fit an organisations specific needs.

A number of factors should be taken into consideration when applying these recommendations, including:

- an organisation's overarching risk assessment,
- the technical platforms already in use, and
- the experience and competence of the operating personnel.

2.1 Managing Zone Content

Content management is defined as how the data published through the DNS is maintained and updated. This can be performed manually (e.g., through a user interface or through direct editing of a text file) or, automatically, based on events in other systems (e.g., DHCP or a directory service). Examples of how these requirements can be met are described more closely in section B.1.

2.1.1 Ensuring Accountability

Accountability requirements should be stipulated to allow updates and other types of changes in the information to be tracked. To facilitate audits, it should also be possible to follow an audit trail of these changes in an existing change management system, and thereby be able to determine the origin and cause of a specific transaction.

[R1] Any change in the configuration and/or data MUST be logged with information about the time of the change, the administrator who performed the change and what information was changed.

[R2] It SHOULD be possible to attach additional information, e.g., a comment or ticket number, to each change.

2.1.2 Revision Control

In addition to knowing who performed what action and when, in many cases, there is a need for being able to go back and compare the information that existed in the system at various times.

[R3] Zone information published in the DNS must be subject for revision control.

[R4] It MUST be possible to roll back and restore data from an earlier revision.

[R5] It SHOULD be possible to show the differences between two different revisions.

2.1.3 Authentication

All system users must be authenticated and use unique, personal system identities. To avoid administrating several sets of system identities, it should be possible to verify these identities and permissions through an external authentication and access control system.

[R6] All users MUST be authenticated when using the system.

[R7] Administrators MUST use personal system identities when accessing the system.

[R8] Authorization SHOULD be administrable through external systems, e.g., LDAP or RADIUS.

[R9] Authentication SHOULD be possible using external systems, e.g., Kerberos, LDAP or RADIUS.

2.1.4 Updating and Editing

Any modification of information published in the DNS should be performed in such a manner that, in addition to meeting the requirements for accountability and access control, the risk of incorrect information being published are also minimized. This can be achieved through syntax validation or peer-review prior to publication.

[R10] The system that is used for updating DNS MUST include syntax validation controls for ensuring that only correctly formatted data can be published.

[R11] The update system SHOULD be able to administer various user permissions, e.g., be able to control which users are permitted to edit specific information.

[R12] The update system MAY have capability to enforce separation of duties through mandatory peer review controls.

2.1.5 Split DNS

A name space is an environment or context in which all names are unique. The largest and most common DNS namespace is the official DNS root administered by ICANN, which applies to the entire Internet. However, some organisations have internal namespaces that are only applicable and accessible within the organisation itself.

Sometimes, there is a reason to return different DNS responses depending on the origin of the query. This may be required if certain information is not to be exposed to external networks or if private IP addresses are used as resources in one part of a network, in parallel with the same resources being reachable via public IP addresses in a different part of the network. At the same time, information that is published in all namespaces must be administered at one single location.

The deployment of DNSSEC puts specific requirements on the administration of split DNS, particularly with regard to key management. In certain cases, it is possible to use the same key material for multiple namespaces, while in other cases it is more appropriate to strictly separate namespaces or, perhaps, leave parts of the namespaces unsigned.

[R13] Split DNS SHOULD be supported by the system.

[R14] DNSSEC for split DNS SHOULD allow configuration to use shared or separate key material for different namespaces. This SHOULD be selectable for each zone.

Where possible, it is often desirable to avoid splitting the namespace in the DNS, thereby simplifying the administration of the DNS. Alternative methods for separating information includes placing resources that are only for internal use in a separate subdomain.

- In modern network architectures, terms such as “inside” and “outside” are often not applicable. Computers and other types of devices are often moved around and, thus, may be used on both internal and external networks, accessing the same resources. Using different addresses for services depending on where a device are connected may complicate the issue significantly.

2.2 Signing and Publishing

The requirements for DNSSEC systems are divided into two distinct parts – the system for key management and the system for signing. Some implementations does not differentiate between these two functions but, since the information can be administered independently, the requirements are presented separately. Examples of how these requirements can be met are described more closely in section B.2.

2.2.1 Requirements for Key Management Systems

The following requirements specify a recommended minimum functional level for a key management system.

[R15] The key management system MUST support separation of keys for key signing (KSK, *Key Signing Key*) and zone signing (ZSK, *Zone Signing Key*).

[R16] The key management system SHOULD support common keys for key signing and zone signing (CSK, *Combined Signing Key*).

[R17] The key management system MUST support key rollover as specified in RFC6781 [20].

[R18] The key management system MUST support automated and scheduled zone signing key rollovers through pre-publishing as specified in RFC6781 [20].

[R19] The key management system SHOULD support key storage in a separate hardware security module (HSM, *Hardware Security Module*).

[R20] If separate hardware security modules are not used, keys MUST be cryptographically protected when stored in persistent system memory.

[R21] The interface between the key management system and any HSMs SHOULD be based on PKCS#11 [23].

2.2.2 Requirements for Signing Systems

The following requirements specify a minimum functional level for a signing system.

[R22] The signing system MUST support DNSSEC in compliance with RFC4033 [13], RFC4034 [15] and RFC4035 [14].

[R23] The signing system MUST support signing with the following algorithms: RSA/SHA-1 as specified in RFC3110 [11], as well as RSA/SHA-256 and RSA/SHA-512 as specified in RFC5702 [19].

[R24] The signing system SHOULD support signing with the following algorithms: ECDSA P-256/SHA-256 and ECDSA P-384/SHA-384 as specified in RFC6605 [18].

[R25] The signing system MUST support NSEC3 as specified in RFC5155 [21].

[R26] The signing system MUST support DS records published with SHA-256 as specified in RFC4509 [17].

[R27] The signing system SHOULD support signing with two or more algorithms simultaneously.

[R28] The signing system SHOULD support signature algorithm rollover without reverting the zone to an unsigned state.

[R29] The signing system SHOULD support transition between NSEC and NSEC3 without reverting the zone to unsigned.

[R30] The signing system MUST support the change of NSEC3 parameters without reverting the zone to unsigned.

[R31] The signing system MUST support the configuration of the signature lifetime.

[R32] The signing system MUST support the configuration of the signature refresh period.

2.3 Distribution

The following requirements specify a minimum functional level for a system for distribution of DNSSEC signed zones. Examples of how these requirements can be met are described more closely in section B.3.

[R33] All zone transfers MUST be protected from modification and truncation.

[R34] Zone transfers SHOULD be protected from modification and truncation through TSIG [25].

[R35] Zone transfers SHOULD be authenticated through use of an algorithm belonging to the HMAC-SHA [12] or GSS-TSIG [25] families.

2.4 Validation

The following requirements specify a minimum functional level for the system for validating DNSSEC signatures. These systems are often deployed as part of a recursive name server (*validating recursive resolver*). Examples of how these requirements can be met are described more closely in section B.4.

[R36] Validation MUST be carried out as specified in RFC4033 [13], RFC4034 [15] and RFC4035 [14].

[R37] Validation MUST support the following algorithms: RSA/SHA-1 as specified in RFC3110 [11] as well as RSA/SHA-256 och RSA/SHA-512 as specified in RFC5702 [19].

[R38] Validation SHOULD support the following algorithms: ECDSA P-256/SHA-256 and ECDSA P-384/SHA-384 as specified in RFC6605 [18].

[R39] Validation MUST support NSEC3 as specified in RFC5155 [21].

[R40] Validation MUST support DS records published with SHA-256 as specified in RFC4509 [17].

[R41] Validation MUST support DNSSEC Opt-In as specified in RFC5155 [21].

[R42] Validation SHOULD support automated updating of trust anchors as specified in RFC5011 [24].

[R43] It SHOULD be possible to turn off validation for the entire or part of the namespace.

2.5 Monitoring

The following requirements specify a minimum functional level for a system monitoring key management, signing and distribution. Examples of how these requirements can be met are described more closely in section B.5.

[R44] The monitoring system MUST check that signatures are updated according to the applicable configuration.

[R45] The monitoring system MUST check that all name servers respond with the correct authenticated positive responses for the zone's SOA, NS and DNSKEY records.

[R46] The monitoring system MUST check that all name servers respond with the correct authenticated denial of existence.

[R47] The monitoring system MUST check that all name servers are updated with current data.

[R48] The monitoring system SHOULD check that all name servers are accurately synchronized with a correct time source.

3 Recommendations for Technical Parameters

This chapter provides recommendations for technical parameters for deployment of DNSSEC at larger organisations and corporations. The parameters are selected based on best current practices and practical experiences from large-scale DNSSEC deployments.

Signing Keys

This guide recommends separation of keys between key signing keys (KSK) and zone signing keys (ZSK) on the grounds that this is currently the most common and well-established model for key management. The signing algorithm used should be RSA/SHA-256, as this is the algorithm that is currently used for the root of the domain name system (DNS). The key lengths for KSK/ZSK should, based on the applicable cryptographic recommendations at the time of writing, be set to 2048 and 1024 bits, respectively.

- KSK: 2048-bit RSA/SHA-256
- ZSK: 1024-bit RSA/SHA-256

Signature Lifetimes

To be able to manage operational disruptions with a healthy margin under, for example, long weekends and holiday periods, this guide recommends that relatively long signature lifetimes are used. This should be combined with daily resigning.

- Signature lifetime: 32 days
- Daily resigning.

Key Rollover

The recommendation is that key material for key signing keys (KSK) are only changed (rolled) when needed, and that any changes of those keys are based on a well-balanced risk analysis. Reasons for changing the KSK could include that personnel who have had access to key material have left the organisation or been given alternative work duties. Procedures for key rollovers should be designed relative to how key material for other systems (e.g., web servers, directory services and terminal services) are administered within the organisation. Rolling the KSK poses a greater risk (compared to rolling the ZSK), as it would normally involve manual intervention, as it requires updating DS-records in the parent zone.

Rolling key material for ZSK can however be handled automatically in most systems. Based on the relatively short key lengths, rollover is recommended every three months.

- KSK rolled as required.
- ZSK rolled every three months (automated).

Method for Authenticated Denial of Existence

NSEC3 is normally used only when one wants to hinder external parties from utilizing exhaustive searches to retrieve all resource records for a zone. The recommendation is to apply NSEC3 for all zones at the level below the top-level domain.

- Negative responses to be authenticated using NSEC3 with 10 iterations.
- Change of NSEC3 salt performed annually, automatically or manually, as supported by the signing system.

Protection of Keys

To reduce the risk of disclosure of key material if, e.g., hardware storing the key material is disposed, lost or stolen, it is recommended that all key material is stored encrypted onto the storage media, even though this may not provide protection against exposure when the system is operational. Key or passphrase for decryption of key material should be stored outside of the system, and provided by the administrator upon activation of the system.

- If possible, all signing keys (KSK/ZSK) should be stored encrypted on storage media, but may be stored unencrypted if the signing system is kept physically protected and adequate procedures for destruction of discarded media are in place.
- Use of a hardware security module (HSM) is not required.

4 Operation and Management

This chapter describes three key stages in the deployment of DNSSEC. These should be managed within the framework of the organisation's standard processes and procedures for IT operation and administration.

4.1 Risk Management

Organisations should have the capability and readiness to manage any risks and incidents that may arise. Such a capability can be built up with the help of training and documented processes and procedures. Documented procedures should be in place for items such as manual resigning, key rollovers and reverting to an unsigned zone in the event of a serious incident.

The main risks introduced by the deployment of DNSSEC relate to the availability of the zone for the validating resolvers. If signatures, keys and parent DS records are not kept up to date, there is a risk that zone data cannot be validated, whereupon the resources published in the zone become unavailable.

A number of interacting measures should be considered to manage and minimize these risks. Among other items, this requires securing the required DNSSEC competence as well as the adaptation of signature lifetimes and key rollover intervals to the specific requirements of that organisation.

4.2 Monitoring

To ensure the zone's availability and to detect and act on errors in early stages, the detailed monitoring of zone data, keys and the condition of signatures is also required. Conditions that should be monitored and compared with each other include:

- the signing function's perception of the current time,
- consistency of the signatures between all of delegated name servers,
- consistency of DS and NS records in the parent zone, and
- consistency of the key records in use.

Monitoring should verify the entire validation chain from DS record to a set of individual resource records within the zone.

4.3 Continuity Planning

Most organisations need a business continuity plan (BCP). The goal is to have in place a preparedness and capability to manage undesirable events that severely impact the availability of information and information resources, and to quickly and systematically manage a crisis situation involving all relevant parts of the organisation. This entails maintaining a preparedness and a capability for managing undesired events including deaths, scandals, fires, production outages, logistical outages, etc. Continuity planning must also ensure that operations can continue, subject to limitations but under controlled conditions, even given interruption of IT support. Continuity planning also includes taking actions to prevent or minimize the effect of undesired events.

In the event that an incident should occur in the management of key material, software and equipment used for DNSSEC, preparedness must be in place to recover from the fault and return to normal operation. Continuity planning includes procedures for managing and replacing compromised or inaccessible key material as well as methods for restarting or changing to an entirely new validation chain.

A Security Policy for DNSSEC

A.1 Introduction

A.1.1 Overview

This appendix formulates a proposal for a security policy for DNSSEC, known as a *DNSSEC Policy (DP)*. A DP sets forth requirements that are appropriate for a specific context or a general specified level of assurance. A DP also constitutes a basis for an audit, accreditation, or another assessment of an entity.

A DNSSEC Practice Statement (DPS), 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 DPs. In other words, the DP says what needs to be done, and the DPS says what is being done.

For example, a regulatory authority may define requirements in a DP for the operation of one or more zones. The DP will be a broad statement of the general requirements for managing the zone. A zone operator may be required to write its own DPS to support the DP, 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 DP, 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.

This DP is adapted for setting definitions of requirements at municipal and regional administrations. It reflects the security-related requirements set out in this guide as well as other additional security aspects arising from a general risk analysis and which also form the basis for existing industry standards in this area.

The structure of the appendix follows the RFC 6841 [22] standard, which provides support for writing a DP. Adhering to this structure facilitates comparison between different DPs, their provisions and their delimitations. The standard also provides support for which topics should be included in a DP, even if certain areas can be left without any provisions.

A.1.2 Document name and identification

Document Name: Kirei 2013:08/A1/en

A.1.3 Community and applicability

This DP formulates a proposal for a security policy for DNSSEC, suitable for adoption at municipal and regional administrations, or other types of similar organisations. It may also be used as support for procurement of DNSSEC-related services.

A.1.4 Specification administration

This document is not updated and only comprises a proposal for a basis for a DP. The document is also expected to be refined and gain support before becoming a policy for DNSSEC deployment.

A.2 Publication and Repositories

A.2.1 Repositories

No separate publishing point is required for information pertaining to DNSSEC in the actual zone, with the exception of that specified in section A.2.2.

A.2.2 Publication of public keys

Public keys that are in use, or which are pending to be taken into use, are only published in the parent zone as DS records.

A.3 Operational Requirements

No stipulation.

A.4 Facility, Management, and operational controls

A.4.1 Physical Controls

Equipment and storage media that contain key material that is in use, or which could come into use, must be stored in a protected area, which can only be accessed by authorized personnel.

A.4.2 Procedural Controls

Access to the signing system may only be granted to individuals whose work duties motivate it and who have undergone the requisite training. Assigned permissions must be reviewed regularly.

A.4.3 Personnel Security

A minimum of two individuals in the organisation are to be assigned responsibility for the system. These individuals must have been given the requisite training to independently and reliably be able to administer the system and perform disaster recovery within the time frame required for maintaining availability of zone data.

A.4.4 Audit logging procedures

All actions taken within the system must be trackable at an individual level and recorded in a security log that includes the time of the action as well as the source and nature of the action. The security log must be protected against tampering and unauthorized access.

A.4.5 Compromise and disaster recovery

A continuity plan must be prepared that includes procedures for managing and replacing compromised or inaccessible key material as well as methods for restarting or rolling to an entirely new validation chain.

The continuity plan and the restart methods must be regularly practiced.

A.4.6 Entity termination

On the termination of operations and if signing is to cease, all key material must be destroyed and any HSM must be zeroized in a controlled manner in line with section A.5.8, Lifecycle management.

A.5 Technical Security Controls

A.5.1 Key pair generation and installation

Keys are to be carefully created in a protected environment, using reliable methods and with a reliable source of random numbers, and where the private component of the key is never stored on non-volatile storage media in an unprotected form.

The transfer, distribution and installation of key material in another environment than where the key material was generated, must be carried out so that the chain of custody of key

material is maintained, and that the confidentiality and integrity of the keys are protected in an appropriate manner given its sensitivity.

Key material that is created for use with DNSSEC may never be used for any other purposes.

A.5.2 Private key protection and cryptographic module engineering controls

The private components of keys used for DNSSEC may never be stored on non-volatile storage media in unprotected (unencrypted) form.

A.5.3 Other Aspects of Key Management

Public components of Key Signing Keys (KSKs) can be archived for a defined period of time for audit purposes.

A.5.4 Activation Data

Activation data that is required for use of private keys must be managed by the designated system administrators responsible for the system.

Activation data must be replaced if one of the designated system administrators leaves their position or is assigned other work duties. The responsibility for this being carried out rests with the immediate superior.

A.5.5 Computer Security Controls

No provisions.

A.5.6 Network Security Controls

The signing system must be logically separated from other systems and networks, and communication between these logical sections must be controlled to ensure that only necessary traffic can flow to and from the system.

A.5.7 Timestamping

The signing system's clock must be continuously synchronized with at least three different reliable sources for standard time traceable to UTC (SP). Synchronization must be monitored.

A.5.8 Life cycle technical controls

New equipment must be tested for a sufficiently long period of time as to ensure its operation for the full duration of a key's lifecycle, before the equipment becomes fully operational. Discarded equipment and media on which active unencrypted key material has been stored must be destroyed before being disposed for recycling.

A.6 Zone Signing

A.6.1 Key lengths, key types and algorithms

The strength of algorithms and key lengths must be selected proportionate to the keys' operational period and the signatures' period of validity. RSA with a modulus length of 2048 bits must be used for keys that will be operational for a period longer than one year, or keys which are used for producing signatures that will be valid for more than one year.

Keys that have been published in parent zones must be allowed an operational period of more than one year and, therefore, the key signing key (KSK) or combined signing key (CSK) must always have a modulus length of 2048 bits.

RSA keys with a modulus length of 1024 bits may be used for operational periods shorter than one year and, accordingly, signatures produced with such keys must also be valid for less than one year.

A.6.2 Authenticated denial of existence

Negative responses are authenticated using NSEC3 with 10 iterations, unless circumstances clearly warrant otherwise.

A.6.3 Signature format

The function for generating the cryptographic hash function used for signing must be selected so that the strength is proportional to the strength of the signing keys.

The algorithm for generating the cryptographic hash must be SHA-256.

A.6.4 Key rollover

Keys that are referred to in parent zones are only changed if suspicion exists of the key being compromised, if the key has been lost or if other circumstances call for a roll-over to other key lengths or algorithms.

The zone signing keys (keys that are not referred to in the parent zone) should be changed every three months using an automated procedure.

A.6.5 Signature lifetime and re-signing frequency

The signature lifetime and resigning frequency must be selected to ensure that the shortest remaining validity period of signatures always exceeds the time it takes for the organisation to reestablish operations in line with the continuity plan.

It is recommended that signature lifetimes to be set to 32 days, and that resigning is performed daily.

A.6.6 Verification of resource records

Where zone data is administered outside of the signing system, the transfer of zone data should be authenticated using strong cryptographic methods, such as TSIG with HMAC-SHA.

A.6.7 Resource records time-to-live

The indicator for the zone data's maximum validity period (*SOA Expire*) must be harmonized with the signatures validity period, so that the zone data in secondary name servers expires before the signature lifetime expires.

The recommendation is that *SOA Expire* is set to 30 days (2,592,000 seconds).

The time-to-live (TTL) of the signature record must be set to the same lifetime as the record the signature covers, and should never exceed one hour.

The TTL for DNSSEC key records (DNSKEY) must be set to a maximum of one hour.

The TTL for authenticated denial of existence (NSEC3) must be set to the same value as that specified for *SOA Minimum*, but never more than one hour.

A.7 Compliance Audit

A.7.1 Frequency of entity compliance audit

Compliance to the security provisions supporting the signing system should be reviewed every two years by an independent internal audit function. The scope and delimitations of the audit should correspond to the scope of this DNSSEC policy. The internal audit should be led by a lead auditor with extensive experience of IT audits. This person can utilize the assistance of technical expertise to verify the effectiveness and efficacy of the controls.

Any deficiencies and their severity must be reported to the manager responsible and an action plan must be prepared. Deficiencies must be rectified promptly when they are of such a nature as to comprise a significantly increased risk. Correction of other types of defects are planned, implemented and followed-up upon in consultation with the involved stakeholders.

A.8 Legal Matters

No stipulation.

B Examples of Technical Controls

This chapter comprises examples of technical controls that can be implemented to meet the requirements set out in chapter 2.

It should be noted that many of the standard products for IP address management and DNS/DHCP (IPAM/DDI) currently available in the market can be used to meet these requirements.

B.1 Managing Zone Content

- By storing all content in a revision control system (e.g., Subversion [6] or GIT [2]) the requirements pertaining to accountability and revision control are complied with – K1, K2, K3, K4 and K5.
- A standard central security log (e.g., *syslog [16]*) server can be used for collection and protection of audit log information – K1.
- Personal system identities linked to a central authentication service (e.g., *Active Directory*) meets the authentication requirements – K6, K7, K8 and K9.
- Automated input controls on checking in new/modified data protects against the risk of publishing incorrectly formatted data – K10.
- The access controls in the revision control system can be utilized to meet the requirement for differentiated user permissions – K11.

B.2 Signing and Publishing

- ZKT [8] and OpenDNSSEC [5] support all MUST requirements applicable to key management – K15, K17 and K18.
- The storage of key material on encrypted file systems (e.g., *TrueCrypt*, *Linux LVM*, *Microsoft Bitlocker*) protects against compromising and tampering when the system is not in operation – K20.
- OpenDNSSEC [5] supports the requirement for storing keys on separate hardware security modules – K19 and K21.
- ZKT [8] and OpenDNSSEC [5] support all MUST requirements applicable to signing – K22, K23, K25, K26, K30, K31 and K32.
- BIND [1] provides fundamental support for combined signing keys (CSK) – K16.
- OpenDNSSEC [5] and BIND [1] supports multiple concurrent signing algorithms – K27.

B.3 Distribution

- BIND [1] and NSD [4] support the protection of zone transfers with the assistance of TSIG/HMAC-SHA256 – K33, K34 and K35.
- Access control for zone transfers does not need to be based on an IP address – the protection provided by TSIG is adequate and, in addition, eliminates the need for the distribution system to know which IP addresses should be provided with access to zone data.

B.4 Validation

- BIND [1] and Unbound [7] support all validation requirements – K36, K37, K38, K39, K40, K41, K42 and K43.

B.5 Monitoring

- Appropriate plug-ins (e.g., for NAGIOS [3]) can be used to meet the monitoring requirements – K44, K45, K46, K47 and K48.

References

[1] BIND. URL: https://www.isc.org/software/bind/.

[2] GIT. URL: http://git-scm.com.

[3] NAGIOS. URL: http://www.nagios.org.

[4] NSD. URL: http://www.nlnetlabs.nl/projects/nsd/.

[5] OpenDNSSEC. URL: http://www.opendnssec.org/.

[6] Subversion. URL: http://subversion.tigris.org.

[7] Unbound. URL: http://www.unbound.net/.

[8] ZKT. URL: http://www.hznet.de/dns/zkt/.

[9] Domain name system — Wikipedia, the free encyclopedia, 2001. [Online; accessed 24-January-2014]. URL: http://en.wikipedia.org/wiki/Domain_Name_System.

[10] Domain name — Wikipedia, the free encyclopedia, 2002. [Online; accessed 24-January-2014]. URL: http://en.wikipedia.org/wiki/Domain_name.

[11] D. Eastlake 3rd. RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS). RFC 3110 (Proposed Standard), May 2001. URL: http://www.ietf.org/rfc/rfc3110.txt.

[12] D. Eastlake 3rd. HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers. RFC 4635 (Proposed Standard), August 2006. URL: http://www.ietf.org/rfc/rfc4635.txt.

[13] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard), March 2005. Updated by RFC 6014. URL: http://www.ietf.org/rfc/rfc4033.txt.

[14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Protocol Modifications for the DNS Security Extensions. RFC 4035 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014. URL: http://www.ietf.org/rfc/rfc4035.txt.

[15] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Resource Records for the DNS Security Extensions. RFC 4034 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014. URL: http://www.ietf.org/rfc/rfc4034.txt.

[16] R. Gerhards. The Syslog Protocol. RFC 5424 (Proposed Standard), March 2009. URL: http://www.ietf.org/rfc/rfc5424.txt.

[17] W. Hardaker. Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). RFC 4509 (Proposed Standard), May 2006. URL: http://www.ietf.org/rfc/rfc4509.txt.

[18] P. Hoffman and W.C.A. Wijngaards. Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC. RFC 6605 (Proposed Standard), April 2012. URL: http://www.ietf.org/rfc/rfc6605.txt.

[19] J. Jansen. Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. RFC 5702 (Proposed Standard), October 2009. URL: http://www.ietf.org/rfc/rfc5702.txt.

[20] O. Kolkman, W. Mekking, and R. Gieben. DNSSEC Operational Practices, Version 2. RFC 6781 (Informational), December 2012. URL: http://www.ietf.org/rfc/rfc6781.txt.

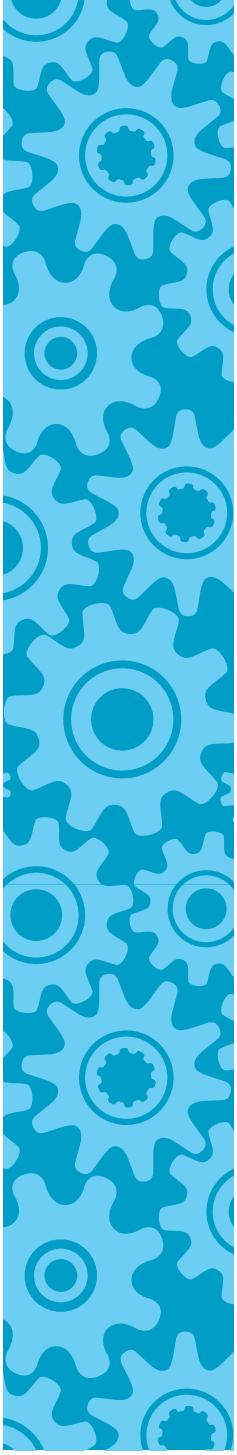
[21] B. Laurie, G. Sisson, R. Arends, and D. Blacka. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. RFC 5155 (Proposed Standard), March 2008. URL: http://www.ietf.org/rfc/rfc5155.txt.

[22] F. Ljunggren, AM. Eklund Lowinder, and T. Okubo. A Framework for DNSSEC Policies and DNSSEC Practice Statements. RFC 6841 (Informational), January 2013. URL: http://www.ietf.org/rfc/rfc6841.txt.

[23] RSA Security, Inc. *PKCS #11: Cryptographic Token Interface Standard*, June 2009. Version 2.30.

[24] M. StJohns. Automated Updates of DNS Security (DNSSEC) Trust Anchors. RFC 5011 (INTERNET STANDARD), September 2007. URL: http://www.ietf.org/rfc/rfc5011.txt.

[25] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington. Secret Key Transaction Authentication for DNS (TSIG). RFC 2845 (Proposed Standard), May 2000. Updated by RFCs 3645, 4635. URL: http://www.ietf.org/rfc/rfc2845.txt.



.SE (The Internet Infrastructure Foundation) is an independent public-service organization with responsibility for the internet's Swedish top-level domain .se, as well as the administration and operation of all of the more than one million domain names on the internet ending with .se. Our surplus is used to finance the continued development of the internet in Sweden, through a number of varied initiatives that contribute in various ways to the development and use of the internet.

The health status of .se is one of these initiatives. The aim of this focus area is, among other things:

- To monitor the quality of the internet's infrastructure in Sweden by compiling and analyzing facts,
- To disseminate the results from surveys, and
- To use advice and recommendations to contribute to ensuring that the infrastructure functions well and has a high level of availability.

Another aim is to, when necessary, detect and inform about deficiencies and improprieties.

.SE (The Internet Infrastructure Foundation)
Box 7399, SE-103 91 Stockholm, Sweden
Tel.: +46 8 452 35 00 Fax.: +46 8 452 35 02
Corp. Reg. No. 802405-0190, www.iis.se

.se
Moving the Internet forward