ZA DNSSEC Policy & Practice Statement Framework

Table of Contents

Chapter 1

Acknowledgements

Portions of this document are attributed to the .SE DPS, licensed under Creative Commons Attribution 2.5 Generic (CC BY 2.5).

The document has been modified and edited to take into account the following characteristics of the ZA zone:

- The lack of a Registry/Registrar model at the second level.
- The lack of Registrants.

1.1 Introduction

This document, known as the ZA DNSSEC Policy & Practice Statement Framework (DPS), provides the parties involved with a statement of security practices and provisions that are applied with respect to DNSSEC in the ZA domain.

This document conforms with the IETF Standard RFC 6841, A Framework for DNSSEC Policies and DNSSEC Practice Statements.

The DPS is one of several documents relevant to the operation of the ZA zone.

1.1.1 Overview

DNSSEC is a set of records and protocol modifications that enable the authentication of DNS data and also make it possible to ensure that content has not been modified during transfer, including mechanisms for authenticated denial of existence.

Resource records secured with DNSSEC are cryptographically signed and incorporate asymmetric cryptography in the DNS hierarchy, whereby trust follows the same chain as the DNS tree, meaning that trust originates from the root and is delegated in the same way as the delegation of a domain. The following IETF RFC’s are referenced in this document:

- RFC 1034
- RFC 1035
- RFC 4033
- RFC 4034
- RFC 4035
- RFC 4509
- RFC 4641
- RFC 5155
- RFC 5702
- RFC 5910

1.1.2 Document name and identification

Title: ZA DNSSEC Policy & Practice Statement Framework

Version: 1.6

Created: 18 May 2016

Updated: 8 December 2016

1.1.3 Community and Applicability

The following roles and delegation of liability have been identified.

ZA Domain Name Authority (ZADNA)

ZADNA bears responsibility for administrating the ZA domain. This means that ZADNA manages supplements, changes, and removal of all data that is related to a domain name delegation. ZADNA generates a zone file and makes it available for AXFR to DNSPL. Once a signed zone is returned from DNSPL, ZADNA publishes the signed zone. ZADNA is responsible for identifying and authenticating the 2nd Level Domain Administrators (2LDAs).

Domain Name Services (Pty) Ltd (DNSPL)

DNSPL is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys. DNSPL retrieves the ZA zone via AXFR. It is then responsible for securely signing all authoritative DNS resource records in the ZA zone. This signed zone is then made available to ZADNA via AXFR for publishing.

DNSPL is responsible for generating DS records based on provided DNSKEY records for each domain.

Finally, the DNSPL is responsible for the secure export and publication of trust anchors (TA) and the registration and maintenance of delegation signer DS resource records in the root zone.

2nd Level Domain Administrator (2LDA)

A 2LDA is an entity that has been delegated a 2nd level domain under ZA. The 2LDA is responsible for generating and protecting their own keys, and registering and maintaining the DNSKEY records through ZADNA. The 2LDA is responsible for issuing an emergency key roll-over if keys are suspected of being compromised or have been lost.

Relying Party

The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate trust anchors. The relying party must also stay informed of any relevant DNSSEC related events in the ZA domains.

Applicability

Each 2LDA is responsible for determining the relevant level of security for their domains. This DPS is exclusively applicable to the top-level ZA domain and describes the procedures and security controls and practices applicable when managing and employing keys and signatures for DNSPL's signing of the ZA zone. With the support of this document, the relying party can determine the level of trust they may assign to DNSSEC in their domain and assess their own risk.

1.1.4 Specification Administration

This document is updated as appropriate, such as in the event of significant modifications in system or procedures that affect the content of the document.

Specification administration organization

Domain Name Services (PTY) LTD

Contact Information

Address: CoZa House, Corporate Park South, Midrand, South Africa

Tel: +27.115682800

Fax: +27.115681492

URL: http://www.dns.net.za

e-mail: info@dns.net.za

Specification change procedures

Amendments to this document are either made in the form of amendments to the existing document or the publication of a new version of the document. This document and amendments to it are published at http://www.nic.za. Only the most recent version of this document is applicable.

ZADNA reserves the right to amend the document without notification for amendments that are not designated as significant. It is in the sole discretion of the specification administrator to designate changes as significant, in which case ZADNA will provide notice. Any changes will be approved by the specification administrator and may be effective immediately upon publication.

1.2 Publication and Repositories

1.2.1 Repositories

ZADNA publishes DNSSEC relevant information on ZADNA's website at https://www.nic.za. The electronic version of this document at this specific address is the official version. Notifications relevant to DNSSEC in ZA domains will be distributed by e-mail.

1.2.2 Publication of public keys

ZADNA will publish KSKs in the form of a DNSKEY and DS as follows:

- ZADNA's website, https://www.nic.za.
- Directly in the root zone (DS Records).

Information published at the specific website is available to the general public and is protected against unauthorized adding, deletion or modification of the content on the website.

1.3 Operational Requirements

1.3.1 Meaning of domain names

A domain name is a unique identifier, which is often associated with services such as web hosting or e-mail, as defined by RFC 1034 and RFC 1035.

Certain restrictions may apply to the new registration of domain names in the ZA Zone.

1.3.2 Identification and authentication of child zone manager

It is the responsibility of ZADNA to securely identify and authenticate the 2LDA through a suitable mechanism, and in compliance with the stipulations in the relationship between ZADNA and the 2LDA.

DNSSEC is activated by a DNSKEY/DS record for the zone being sent from the 2LDA to ZADNA and a DS record being generated and published in the DNS, which establishes a chain of trust to the child zone.

No controls are conducted with the aim of validating DNSKEY/DS Records, and it is the responsibility of the 2LDA.

1.3.3 Registration of delegation signer (DS) resource records

ZADNA accepts DNSKEY or DS records through the EPP interface from each 2LDA, or alternatively via some other agreed secure method. The DS record is then generated from the DNSKEY if provided. The DNSKEY record must be valid and sent in the format indicated in RFC 5910 (EPP DNS Security Extensions Mapping), or as per another agreed secure format.

1.3.4 Method to prove possession of private key

ZADNA does not conduct any controls with the aim of validating the 2LDA as the manager of a private key. The 2LDA is responsible for conducting the controls deemed necessary.

1.3.5 Removal of DS record

A DNSKEY record is de-registered by issuing the relevant EPP DNSSEC update command, or as per another agreed secure authenticated format. The de-registration of the DNSKEY/DS records will deactivate the DNSSEC security mechanism for the zone in question.

Who can request removal

Only the 2LDA, or the party formally designated by the 2LDA, has the authority to request de-registration of the DS records.

Procedure for removal request

The 2LDA or the 2LDA's representative tasks ZADNA with implementing the de-registration. From the time the de-registration request has been received by ZADNA via the EPP protocol, or other agreed secure format, it takes no longer than until the next zone generation for the change to be recorded in the zone file. Subsequently, it takes the TTL (15 minutes) plus the distribution time before the changes have been deployed. The whole procedure may take a maximum of 2 hours to complete.

1.4 Facility, Management and Operational Controls

1.4.1 Physical Controls

ZADNA has implemented physical security controls to meet the requirements specified in this document.

Site location and construction

ZADNA will establish two fully operational and geographically dispersed operation centres. The redundant facility will contain a complete set of ZADNA's critical systems, whose information will be continuously updated through automatic replication of the normal operations facility. All of the systems components will be protected within a physical perimeter with an access control and alarm system contracted by ZADNA.

The backup operations facility meets the minimum standards applied to the normal facility in terms of physical security, power supply, environment, and fire/water protection.

Physical access

Physical access to the protected environment will be limited to authorized personnel. Physical access is restricted by key cards. Entry is logged and the environment will be continuously monitored. Online HSMs are protected by locked cabinets and offline HSMs will be protected through the use of locked safes.

Power and air conditioning

In the event of power outages, power will be provided by UPS until the backup power systems have begun to generate electricity. The backup power systems will have the capacity to supply critical resources with electricity. Air conditioning systems will be redundant.

Water exposures

The facilities will implement flooding protection and detection mechanisms.

Fire prevention and protection

The facilities will be equipped with fire detection and extinguishing systems. The facilities will be equipped with automatic extinguishers with dry extinguishing.

Media storage

ZADNA’s guidelines for information classification define the requirements imposed for the storage of sensitive data.

Waste disposal

Disposed storage media and other material that may contain sensitive information will be destroyed in a secure manner, either by ZADNA or by a contracted party.

Off-site backup

Certain critical data will also be securely stored using a off-site storage facility. Physical access to the storage facility will be limited to authorized personnel. The storage facility will be geographically separate.

1.4.2 Procedural Controls

Trusted roles

Trusted roles are held by persons that are able to affect the zone file's content, delivery of trust anchors or the generation or use of private keys. The roles are appointed by DNSPL. The trusted roles are:

- Systems Administrator (SA).

- Security Officer (SO).

In addition to the two operational trusted roles, there is a third non-operational role of Security Watcher (SW). The role of the SW is to observe the processes and procedures employed by SO and SA. The SW is appointed by ZADNA and their attendance at signing processes is optional.

Number of persons required per task

At any given time, there must be at least two individuals within the organization per trusted role indicated in Trusted roles. Key generation requires two people to be present; one from each role.

The export and control of trust anchors requires two people to be present; one from each role.

None of the aforementioned operations may be performed in the presence of unauthorized people.

A SW can be present in a non-operational, observation role.

Identification and authentication for each role

Only people who have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with DNSPL may hold a trusted role. Before a person receives their credentials for system access, a valid form of identification must be presented.

Tasks requiring separation of duties

The trusted roles in Trusted roles above may not be held simultaneously by one and the same person.

1.4.3 Personnel Controls

All Personnel must have valid employment contracts which address their duties with regards this DPS.

1.4.4 Audit Logging Procedures

Logging is automatically carried out and involves the continuous collection of information regarding the activities that take place in an IT system. The logged information is used in the monitoring of operations, for statistical purposes and for investigation purposes in suspected cases of violation of this DPS. Logging information also includes the journals, checklists and other paper documents that are vital to security and that are required for auditing. The purpose of the collected log information is to be able to reconstruct the case after-the-fact and analyse which people or applications/systems did what and at what time. Logging and the identification of users enables such features as traceability and the follow-up of unauthorized use.

Retention period for audit log information

Log information is stored in log systems for not less than 30 days. Thereafter, the log information is archived for not less than 5 years. Database table audit logs will persevere for a minimum of 5 years.

1.4.5 Compromise and Disaster Recovery

Incident and compromise handling procedures

All real and perceived events of a security-critical nature that caused or could have caused an outage or damage to the IT system, disruptions and defects due to incorrect information, or security breaches are defined as incidents. All incidents are handled in accordance with DNSPL's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, what effects the incident has had or may have had, measures to prevent the incident from recurring and forms to further report this information. An incident that involves suspicion that a private key has been compromised leads to the immediate roll-over of keys pursuant to the procedures indicated in private key compromise procedures.

Corrupted computing resources, software, and/or data

In the event of corruption, the incident management procedures shall be initiated and appropriate measures shall be taken.

Entity private key compromise procedures

Suspicion that a private key has been compromised or misused leads to a controlled key roll-over as follows:

- If a Zone Signing Key (ZSK) is suspected of having been compromised, it will immediately be removed from production and stopped being used. If necessary, a new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or timed out. If a ZSK is suspected of having been compromised is revealed to unauthorized parties, this will be notified through the channels indicated in Repositories.
- If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents. A KSK rollover in progress is always notified through the channels indicated in Repositories.
- If a KSK is lost, a new key will be generated with new DS record. A request to IANA to publish the additional DS corresponding to the new KSK will be issued. Once IANA changes are propagated, the old DNSKEY is taken out of service and swapped for the new DNSKEY. At such time, the change is announced using the mechanisms defined in Repositories. During the time preceding the roll-over, the key set remains static and any scheduled ZSK roll-over is postponed until the KSK swap is complete.

1.4.6 Entity termination

If ZADNA must discontinue DNSSEC for the ZA zone ,without transferring operations to another party, for any reason and return to an unsigned position, ZADNA will be responsible for informing relevant stakeholders and the general public in an orderly manner. If the DNSSEC operations are to be transferred to another party, DNSPL will participate in the transition so as to make it as smooth as possible, as per the Service Orders between ZADNA and DNSPL.

1.5 Technical Security Controls

1.5.1 Key Pair Generation and Installation

Key pair generation

Key generation takes place in a hardware security module HSM that is managed by trained and specifically appointed personnel in trusted roles. Key generation takes place when necessary and is performed by the software.

Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SO and SA. The SO is responsible for publishing the public component of the KSK in a secure manner as per Repositories. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

Public key parameters generation and quality checking

Key parameters are regulated by DNSPL's KASP (Key and Signing Policy) and quality control includes checking the key length.

Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system. A signature that is created by a DNSSEC key for either a ZSK or a KSK. A ZSK never has a longer validity period of more than 32 days (30 days plus two days of jitter), and this validity period always begins when the temporary signature has been established. A KSK is valid for one year.

1.5.2 Private key protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed in the hardware module and no private keys are ever found unprotected outside an HSM.

Cryptographic module standards and controls

The system uses a hardware security module HSM which conforms to the requirements in FIPS 140-2 level 3.

Private key (m-of-n) multi-person control

DNSPL does not apply multi-person controls for HSM activation.

An SO and a SA is required to activate the module, which in turn requires physical access, which can only be performed by the SA.

Private key backup

The key archive is encrypted with a Storage Master Key SMK. The master key is stored on a portable storage medium in a secure environment, which can only be accessed by an SO. Keys are stored in an encrypted format on the signing module's hard drive. The encrypted key archive is securely backed up and synchronized between the operations facilities on a daily basis or immediately following a key generation.

Private key storage on cryptographic module

The Storage Master Key SMK is shared by all security modules in the system.

The master key is used to decrypt the key archive that is stored outside the security module while deactivated.

Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

Private key transfer into or from a cryptographic module

During the installation of the signing system, a joint HSM key (or Storage Master Key, SMK) is transferred via a portable USB media, after which the HSM is locked to prevent further export of keys. The USB media is subsequently stored in accordance with Private key backup.

Method of activating private key

Private keys are activated by unlocking the HSM. An SA provides an SO with access to the facility. The SO states a personal passphrase for the HSM through a console.

Method of deactivating private key

The HSM is locked if the signing system is either turned off or rebooted.

Method of destroying private key

Private keys are not destroyed. After their useful life, they are removed from the signing system.

1.5.3 Other Aspects of Key Pair Management

Public key archival

Public keys are archived in accordance with the archiving of other information relevant to traceability in the system, such as log data.

Key usage periods

Keys become invalid as they are taken out of production. Old keys are not reused.

1.5.4 Activation data

The activation data is the personal pass-phrase for each SO that is used to activate the HSM.

Activation data generation and installation

Each SO is responsible for creating their own activation data pursuant to the applicable requirements of at least nine characters of varying nature.

Activation data protection

Each SO is responsible for protecting their activation data in the best possible way. On the suspicion of compromised activation data, the SO must immediately change it.

Other aspects of activation data

In the event of an emergency, there is a sealed and tamper evident envelope in a secure location that contains activation information with instructions on appointing an Emergency Security Officer (ESO). ZADNA's DNSSEC contingency plan procedures state the conditions in which this shall be applied.

1.5.5 Computer Security Controls

All critical components of ZADNA and DNSPL's systems are placed in secure facilities in accordance with Physical Controls. Access to the server's operating systems is limited to individuals that require this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

1.5.6 Network Security Controls

Networks are logically sectioned and are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. All sensitive information that is transferred over the communications network is always protected by strong encryption.

1.5.7 Timestamping

The systems retrieve time that is traceable to timeservers from africa.pool.ntp.org. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

1.5.8 Life Cycle Technical Controls

System development controls

All source code is stored in a version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe. ZADNA's development model is based on industry standards and includes:

- Fully functional specification and documented security requirements,
- Documented architectural design based on a natural modularization of the system,

- Continuous pursuit of minimizing complexity,
- Systematic and automated testing and regression tests,
- Issuing of distinct software versions,
- Issuing Version Control Tags upon release
- Constant quality follow-ups of detected defects.
- Constant reliability follow-ups
- Post-delivery maintenance

Security management controls

Authorization registers are kept and followed up regularly. DNSPL also conducts regular and ad-hoc security audits of the system. DNSPL prepares and maintains a system security plan that is based on recurring risk analysis.

1.6 Zone Signing

1.6.1 Key lengths, key types and algorithms

Key lengths and algorithms are to be of sufficient length for their designated purpose during each key's useful life. Algorithms shall be standardized by the IETF, available to the public and resource efficient for all parties involved.

The RSA algorithm with a key length of 2048 bits is currently used for KSK and 1024 bits for ZSK.

1.6.2 Authenticated denial of existence

The signing uses NSEC3 records as specified by RFC 5155, and may sort zones prior to signing, in order to maximize NSEC3 efficiency.

1.6.3 Signature format

Signatures are generated using an appropriate cryptographic hash function.

1.6.4 Key roll-over

ZSK rollover is carried out every 28th day with a pre/post period of 7 days either side for new/old keys respectively.

1.6.5 Signature life-time and re-signing frequency

RR sets are signed with ZSKs with a validity period of between six and eight days. Re-signing takes place every other odd UTC hour.

1.6.6 Verification of Zone Signing Key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. The above mentioned is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the ZA Start Of Authority (SOA).

1.6.7 Verification of resource records

The resource records are verified as valid in accordance with the current standards prior to distribution.

1.6.8 Resource records time-to-live

Controlled using the Key And Signing Policy (KASP). RRSIG inherits TTL from the RR set that it signs.

1.7 Compliance Audit

Audited documents (policy, procedures, requirements), information regarding facts or other information that is relevant in consideration of the audit criteria and that is verifiable are used as documentation when conducting audits.

1.7.1 Frequency of entity compliance audit

The need for audits is decided and paid by ZADNA. Circumstances which may entail an audit requirement are:

- Recurring anomalies.
- Significant changes that are made at the management level, in the organization or in processes.
- Other circumstances, such as the competence among personnel, new equipment or other major changes.

1.7.2 Identity/qualifications of auditor

The auditor shall be able to demonstrate proficiency in IT security, DNS and DNSSEC.

1.7.3 Auditor's relationship to audited party

An external auditing manager shall be appointed for the audit. When necessary, the auditing manager shall be able to recruit specific expert knowledge. The auditing manager is responsible for implementation during the entire audit.

1.7.4 Topics covered by audit

The auditing manager's assignment includes ensuring that:

- The right competence represents ZADNA.
- The auditee is informed and prepared prior to the audit.
- The auditee is informed of the topic of the audit in advance.
- Follow-up procedures of the audit results are in place.

1.7.5 Actions taken as a result of deficiency

The auditing manager shall immediately verbally inform ZADNA's management of any anomalies.

1.7.6 Communication of results

The auditing manager shall submit a written report of the audit results to ZADNA not later than 30 calendar days after the audit.

1.8 Legal Matters

1.8.1 Fees

No fees will be charged by ZADNA for DNSSEC.

1.8.2 Privacy of personal information

Responsibility to Protect Personal Information

Regulated by ZADNA's agreement with 2LDAs.

Disclosure of Personal Information to Judicial Authorities

Decisions regarding the disclosure of personal information to judicial authorities may be made upon direct request. The matter of disclosure is decided case-by-case. Decisions are made by ZADNA's legal department.

1.8.3 Limitations of liability

Liability of damage between ZADNA and DNSPL is regulated by contract. ZADNA's liability of damage toward the 2LDAs is regulated by the agreement between them.

1.8.4 Term and termination

Validity Period

This document applies until further notice.

Expiration of Validity

This document does not expire but can be replaced by newer versions.

Dispute Resolution

Any dispute or conflict resulting from this Agreement shall be filed at any South African Court.

Governing Law

South African law applies to the actions under this DPS.