DNSSEC Policy & Practice Statement for .tz Zone

Version 1.1

Effective Date: January 1, 2013

Tanzania Network Information Centre
14107 LAPF Millenium Towers, Ground Floor, Suite 04
New Bagamoyo Road, Dar es Salaam,
Tanzania.
+255 22 2772659
http://www.tznic.or.tz

1 Introduction

This document is the Tanzania Network Information Centre (tzNIC) DNSSEC Policy and Practice Statement for the .TZ zone and its second level domains. It states the practices and provisions that tzNIC employs in providing .TZ zone signing and distribution services that include, but are not limited to, issuing, managing, changing and distributing DNS keys. This document conforms to the RFC-draft DNSSEC Policy & Practice Statement Framework (version 03).

1.1 Overview

DNSSEC is an extension to the Domain Name System that allows data retrieved from the DNS to be authenticated. DNSSEC as intended for use for names in the .TZ domain is specified in RFC 4033, RFC 4035 and RFC 5155.

DNS Resource Records secured with DNSSEC are signed cryptographically using asymmetric techniques. The public keys corresponding to private keys used to sign data are published in the DNS itself as signed resource records. One or more trust anchors for the .TZ zone are published in the DNS as Delegation Signer (DS) Resource Records in the root zone. Trust in signatures published in the .TZ zone can consequently be inferred from the trust in signatures in the root zone.

1.2 Document name and identification

Document title: DNSSEC Policy & Practice Statement (DPS)

Version: 1.1

Created: June 28, 2012

1.3 Community and Applicability

tzNIC, a registry operator of .tz name space conforms with registry-registrar-registrant model, however, tzNIC still uses a registry-registrant model which will be phased out once the full 3R model is adopted. The following are the roles and functions that have direct impact to the deployment of DNSSEC.

1.3.1 TZ Registry

Tanzania Network Information Center (tzNIC) operates the .TZ registry. tzNIC is responsible for managing the .tz registry and consequently for registration of domain names under the .TZ second level domains.

tzNIC is responsible for adding and removing records in the .tz zone as well as all the associated second-level domains. It is also responsible for generating, sign and store the Private and public cryptographic keys used to sign .tz zone as well as all the other second-level domains.

1.3.2 TZ Registrars

Registrars are the entities that have been accredited by the tzNIC and they are given a mandate to

register and manipulate domains on behalf of the registrants. The registrars use an EPP enabled system to perform different operations in the registry. Their operations on the registry affect the zone file of second level domains.

Registrars are responsible for adding, removing or updating Delegation Signer (DS) records for each domain at the request of the domain's registrant.

1.3.3 TZ Registrants

Registrant is a physical or legal entity that has a mandate and has all the rights over a particular domain. Registrant is responsible for securing his domain by generating cryptographic key pairs, signing the zone of his domain , securing the cryptographic keys and maintaining the DS of the domain on the registry through a registrar.

1.3.4 Other Parties

These are all other parties that support the security that is provided by DNSSEC. These includes all the operators of validating resolvers that need to properly create and update the DNSSEC trust anchor and configurations.

1.4 Specification and Administration

This document .tz DNSSEC policy and practice statement will be reviewed and updated periodically as tzNIC receives comments from Internet community and as per proposed changes in Internet drafts.

1.4.1 Specification Administration Organization

Tanzania Network Information Center (tzNIC)
14107 LAPF Millennium Towers, Ground Floor, Suite #4,
New Bagamoyo Road,
Dar es Salaam, Tanzania.

1.4.2 Contact Information

Administrative Manager
Tanzania Network Information Center
14107 LAPF Millennium Towers, Ground Floor, Suite #4
New Bagamoyo Road
Dar es Salaam, Tanzania.
Phone: +255 222 772 659
Fax: +255 222 772 660
Email: info@tznic.or.tz
Website: www.tznic.or.tz

1.4.3 Specification Change Procedures

Changes to this document can either be in form of amendments to this document or publishing a new document. At any time the current operating DNSSEC policy and practice statement document will be available at < http://www.tznic.or.tz/knowledgebase/dnssec/ >.

All changes to this document will be approved by tzNIC and become effective immediately upon its publication. Tanzania Network Information Center (tzNIC) reserve the rights of amendment of this document at any time without a prior notification of amendment.

2 Publication and Repository

2.1 Publication Site

All information related to DNSSEC will be published in the tzNIC website at < http://www.tznic.or.tz/knowledgebase/dnssec > and all notifications will be distributed by email to dnssec-announce@tznic.or.tz.

2.2 Publication of Key Signing Key (KSK)

The key signing key (KSK) will be published in the form of DS record in the root zone. This key will also be published in the tzNIC website < http://www.tznic.or.tz/knowledgebase/dnssec/ksk >

2.3 Access Control

All the DNSSEC-relevant information will be published in tzNIC website and the information will be accessible to the general public. This information is protected against unauthorized editing i.e. adding, deletion or modification of the content.

3 Operational Requirements

3.1 Meaning of a domain

A domain is unique identifier in the DNS, as described in RFC 1034 and RFC 1035. For the purpose of this document a domain name is a name registered under the .TZ second-level domains, and corresponds to a delegation from .TZ zone to name servers operated by or on behalf of the domain name's registrant. A .tz domain can be obtained by any legally existing organization or company on first come first served and as per tzNIC rules for domain registration.

3.2 Activation of DNSSEC for child zone

For a child zone to activate DNSSEC, at least one DS record must be uploaded by the registrar to the registry and subsequently published on the DNS zone to establish a chain of trust.
The registry will not check the validity of the DS record and will assume the DS record is correct and is in a proper format.

3.3 Identification and Authentication of Child-zone Manager

It is the responsibility of the registrar to identify an authenticate a child zone manager or in other words a registrant through a suitable mechanisms as per rules and regulations set by the registry.

3.4 Registration of Delegation Signer (DS)

The DS records or in other words a Delegation signer is used to establish a trust anchor. This is accepted by the registry through an EPP interface from a registrar. The DS must be valid and will have to conform with RFC 4310.

3.5 Method to prove possession of Private Key

The registry does not conduct any controls to validate the registrant as the owner of the private key. The registrar is the one that is supposed to establish the controls in place to validate the private keys of the registrant.

3.6 Removal of DS records.

The removal of DS record is performed by a registrar using an EPP system to modify the zone file for a particular domain. This removal deactivates DNSSEC for the particular domain. The removal request can only be made by the owner of the domain designated as a registrant or the technical contact/administrative contact under the approval of registrant. The registrar will implement the modification and the effect in the zone file will take place in the next zone generation. The time it takes for the deployment to take place depends on the TTL and the distribution time the zone. In a circumstance of an emergency and the registrant can not reach the registrar, the registry can make the removal of the DS record for the registrant after validating the identity of the registrant.

4 Facility, Management and Operational Controls

4.1 Physical Controls

Based on continuous risk analysis and re-evaluation of threats, tzNIC implements physical protection,monitoring and access controls, as well as appropriate compensating controls, to reasonably ensure that the registry and signer systems are not tampered with.

4.1.1 Site location and Construction

The registry has two operations centers that are 4.7 km apart. The redundant location contains all the necessary and critical systems for the functioning of the registry and it is updated in realtime so that all the data available in the main site is also available at the redundant site.

4.1.2 Physical Access

The access to the two operating centers is restricted to authorized personnel only and the access is digitally logged and the the room is constantly monitored.

4.1.3 Power and Air Conditioning

Power to the the two centers is provided by the commercial power, a generator, Electric Inverter as well as UPS. In an event of disruption of commercial power, an automatic generator will service the center, and in an event where the generators can not do that then the Inverter will server the facilities.

4.1.4 Fire Protection and Prevention

The registry operating facilities are equipped with fire detection mechanisms and they are able to extinguish fire incidents that happen in the operating facilities.

4.1.5 Media Storage

All the sensitive data stored in movable storage devices are stored in a fireproof safe and can only be accessed by authorized personnel.

4.1.6 Water Exposure

In an event of flooding of our primary site, the secondary site can take over and perform the tasks of the primary site.

4.1.7 Waste Disposal

All the sensitive information have to be properly disposed in a secure manner to avoid information leakage.

4.1.8 Off-site Backup

All the sensitive data are backed up in a tape drive and stored in an off site facility.

4.2 Procedural Controls

4.2.1 Trusted Roles

These are DNSSEC experienced staff that are well trained and are tasked to perform DNSSEC related activities including generation of cryptographic keys, managing the trust anchor etc. The roles include:-

1.Systems Administrator, SA.
2.Security Officer, SO.

4.2.2 Number of Persons required per Tasks

There should be at least two people responsible for the role of Systems Administrator SA and Security Officer SO when performing DNSSEC related activity on the DNSSEC signer system.

4.2.3 Identification and Authentication of People in Trusted Roles

Any person who holds the SA and SO roles must first sign the confidentiality agreement and an agreement to acknowledge their responsibilities. The agreement is exchanged with the Signing system credentials.

4.2.4 Separation of Duties

It is discouraged for the above two roles to be carried by one individual. The best practice will be for the two roles performed by two different individuals.

4.3 Personnel Controls

4.3.1 Qualifications and experience

An individual seeking to be recruited to either of the two trusted roles must have the qualifications as per the ones set by tzNIC. The individual will have to present his/her certificates to prove the qualifications possessed.

4.3.2 Background check procedures

The registry will do the background check to verify the individual's capacity to assume/hold either the SO or SA roles.

4.3.3 Training requirements

tzNIC understands the importance of the technical competence within the trusted roles and will continue to train the individuals holding the trusted roles to equip them with the necessary skills to assist them in the proper management of DNSSEC. With the changing technology the registry will try to keep up by training the trusted roles so as to secure the DNSSEC and the registry platform in general.

4.3.4 Job rotation frequency and sequence

As one of the security control, the registry will keep performing job rotations between the trusted roles. This will assist the individuals holding the roles to have experience of the role hold by another individual.

4.3.5 Sanctions for unauthorized actions

All the sanctions of unauthorized actions on the signing systems and improper use of the credentials are penalized as per the signed responsibility agreement. Severe negligence or activities may lead to termination.

4.3.6 Contracting personnel requirements

In an event where by the registry requires contractors to perform registry related activities, the

contractors will have to sign confidentiality agreement and responsibility agreement. Contractors whose background has not been thoroughly reviewed shall not be granted any trusted role.

4.4 Audit Logging procedures

The registry DNSSEC signing system does keep logs automatically. These logs are used to trace the event that occurred, trace the error in the systems and also used to generate different types of statistics.

4.4.1 Types of events recorded

The following activities are logged :-

1.All the signing related activities are logged in the signing systems. This includes zone signing and re-signing.
2.All the activities performed in the HSM including keys generations, keys rollover are logged.
3.All successful and unsuccessful attempts to the signing systems are logged.
4.All privileged operations and physical access to the facilities are logged.

4.4.2 Frequency of processing log

The logs in the DNSSEC signer system shall be automatically and manually analyzed from time to time.

4.4.3 Retention period for audit log information

Log captured in the systems are retained for at least 30 days and thereafter archived for at least a year.

4.4.4 Protection of audit log

All the logs captured in the DNSSEC signing system are only accessed by the authorized individuals who do not have access to erase or overwrite them.

4.4.5 Audit log backup procedures

All the logs are backed up on external backup tapes and stored in a distant secure location.

4.4.6 Audit collection system

All the electronic logs are transferred in real-time to a logs collection system. In a logs collection system, the logs are also protected from unauthorized access.

4.4.7 Vulnerability assessments

All abnormal activities are investigated so as to identify any potential vulnerabilities.

4.5 Compromise and Disaster Recovery

4.5.1 Incident Management Procedures

In case of a security incident, a proper incident management procedure will be followed as per Incident Management procedure set by the registry. In a scenario of a private part of KSK being compromised or likely to have been compromised, the registry will initiate an emergency key rollover of the KSK.

4.5.2 Corrupted equipment , software or information

In case of a hardware failure, the failed hardware will be replaced as soon as possible by the responsible vendors. With software failure, the registry ensures the recovery of the software as per recovery procedure of the particular system.

4.5.3 Business continuity and Disaster Recovery

The registry ensures resumption of the disrupted services as soon as possible to the secondary facility in case of the primary site is affected by any disaster.

4.6 Entity Termination

In case it is necessary for the registry to terminate the DNSSEC services due to any reasons, the registry will perform the rollback in a controlled, secured and orderly manner. In a situation where the registry's operations are transfered to another organ, the registry will cooperate with the transfer in a proper and systematic way to avoid any technical glitches to the registrants.

5 Technical Security Controls

5.1 Key pair generation and installation

5.1.1 Key pair generation

Key pair is generated by the hardware security module and the task is handled by the well trained trusted roles. The key generation procedure is logged electronically and documented manually.

5.1.2 Public key delivery

The KSK is then copied automatically to the backup facility for storage. The security officer is then responsible for publishing the DS record in the root zone.

5.1.3 Public key parameters generation and quality checking

The key parameters are managed under the key and signing policy and the quality requires checking the key length.

5.1.4 Key usage purpose

The keys that are generated for DNSSEC should only be used for DNSSEC and nothing else. All the keys should never be reused but should be used only once.

5.1.5 Other aspects of key pair management

The KSK will be rolled over once in two years and the ZSK will be rolled over after every two months. All the obsolete keys will never be stored and backed up but rather will be removed from the signing system.

5.2 Computer security controls

The DNSSEC signing system is managed under the registry IT security policy where by all the access and activities in the system shall be logged. All the equipments used in the DNSSEC signing system are placed in a secure facility.

5.3 Network security controls

The network facility of the DNSSEC signing systems is properly isolated and all activities are logged in a firewall. All the data transfered across the network is encrypted with strong encryption.

5.4 Time stamping

All the server and other equipments in the registry and the DNSSEC signer system are synchronized with Stratum Time servers and the time stamps are in UTC.

5.5 Life cycle technical controls

DNSSEC will be implemented by using OpenDNSSEC. A new version of openDNSSEC is first tested in a testbed before being deployed as per predefined procedures.

6 Zone Signing

6.1 Key lengths and algorithms

The key size of 2048 bits for KSK shall be used and 1024 bits for ZSK shall be used and the algorithm is RSA.

6.2 Authenticated denial of existence

The registry shall use NSEC records to authenticate denial of existence as specified in RFC 4034.

6.3 Signature format

The zones will be signed with signature generated using RSA operation over a cryptographic function with SHA1.

6.4 Zone signing key rollover (ZSK)

The zone signing key (zsk) shall be rolled over after every 60 days.

6.5 Key signing key rollover (KSK)

The key signing key shall be rolled after every two years under normal circumstances else it shall be rolled over when needed.

6.6 Signature life-time and resigning frequency

The signature life time shall be of seven (7) days and zones shall be resigned after every one (1) hour.

6.7 Verification of zone signing key set

The validity period of keys and security controls are checked against the DNSKEY before publishing the zone information on the Internet. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the SOA.

6.8 Verification of resource records

The registry shall verify the RR Sets to make sure they conform with the current standards before publishing the zone.

6.9 Resource records time-to-live (TTL)

The TTL for DS records, DNSKEY and NSEC records will be set to 3600 seconds. RRSIG records inherit TTLs from the corresponding signed RR set.

7 Compliance Audit

The DNSSEC systems, services and procedures shall be audited from time to time. The audit report shall be presented to the registry management, Policy Advisory Committee and subsequently to the members meeting (AGM). The recommendations of the auditor shall be taken into account so as to enhance security of the DNSSEC systems.

8 Legal Matters

8.1 Fees

No fees are charged for any function related to DNSSEC.

8.2 Financial Responsibility

tzNIC accepts no financial responsibility for improper use of Trust Anchors or signatures, or any other improper use under this DPS.

8.3 Term and Termination

This DPS applies until further notice.

8.3.1 Term

This DPS is valid until it is replaced by a new version.

8.3.2 Termination

This DPS is valid until it is replaced by a new version.

8.3.3 Dispute Resolution Provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

8.3.4 Governing Law

This DPS shall be governed by the laws of Tanzania applicable therein.