East African Communications Organisation

Communications for all in East Africa

EACO MODEL GUIDELINES FOR DEPLOYMENT OF DOMAIN NAME SYSTEM SECURITY (DNSSEC)

Prepared by EACO
July 2021

CONTENTS

ACRONYMS

BCP	Best Current Practice
ccTLD	country code Top Level Domain
DPS	DNSSEC Practice Statement
DNS	Domain Name System
DNSSEC	DNS Security Extensions
IP	Internet Protocol
ISP	Internet Service Provider
TISPA	Tanzania Internet Service Providers Association
tzNIC	Tanzania Network Information Center

EACO GUIDELINES FOR DNSSEC DEPLOYMENT

1 DOMAIN NAME SYSTEM

The Domain Name System (DNS) is analogous to the "address book" of a Cellular phone. Similar to using the address book to look up a name in order to find a phone number, you look up a domain name in DNS to find an IP address. IP addresses and domain names are affiliated.

All computing devices linked to the Internet have their own IP address (IPv4 or IPv6) which makes it possible to connect to one another. However, to save users from having to remember these long strings of numbers, DNS attaches a unique domain name to the IP address. When you look up a domain name, a search for an IP address is initiated in order to contact the server hosting the service you are looking for. Each domain name is linked to a series of computers which respond to enquiries regarding addresses registered within the domain name. These computers are called *name servers*. For the most part, the user is unaware of communication with these computers.

An example of a typical query is explained below:

You want to look up a specific event posted on the University of Dar es Salaam website. You know that the university's address is www.udsm.ac.tz so you enter this in the address field of your browser.

1. A small software application in your computer contacts a separate computer – a so-called "recursive resolver" – which has been set up to process enquiries made to the domain name system. This computer is usually located on the premises of the Internet Service Provider (ISP) or the University itself.
2. The job of the recursive resolver is to find the IP address for *www.udsm.ac.tz*. It sends the enquiry onwards to one of the name servers for the root in the domain name system. The root name servers recognize only the level below them in the hierarchy and so send back a list of the name servers for *.tz*.
3. The resolver then re-sends the same enquiry to one of the name servers for *.tz*. Fortunately, these servers are designed to recognize two levels below them, and so send back a list of the name servers for *ac.tz*.
4. The resolver repeats the enquiry to one of the name servers for udsm.*ac.tz*, which responds with the IP address for www.udsm.ac.tz
5. The resolver then sends the IP address to your computer. When your browser receives the address, it can then contact the university's web server and download the website wanted.

2 WHAT IS DNSSEC?

When you look up a domain name, a call for an IP address initiates a search in DNS, which is used to contact the server hosting the service that you want to access. Basically DNS does not secure that an answer comes from the correct source of origin. This means that a scammer may falsify an answer and lead you to another IP address than the one affiliated to the domain. You may for example be lead to a website looking similar to the website you tried to reach, but the site is actually run by a server controlled by a scammer.

"DNS Security Extensions," commonly known as DNSSEC, provide a way to authenticate DNS response data. Before you connect to a website, your browser has to retrieve the IP address of the site using DNS. However, it is possible for an attacker to intercept your DNS queries and provide false information that would cause your browser to connect to a fake website where you could potentially provide personal information (for example, what you think is a bank website). DNSSEC provides a level of additional security where the recursive resolver check to confirm that the answer (in this case IP address) received comes from the right source and was not modified. Verification is done by the recursive DNS server, and not the web browser.

When a domain is DNSSEC secured, all answers to lookups will be cryptographically signed. This makes it possible to check that the reply to the lookup comes from the correct source of origin, and that the lookup remains unchanged.

The signature is made by means of a private key, which is available only to the one running the domain. The signature is checked by the server doing the lookup in DNS, which then fetches the public key for the domain. Then the key and the signature are combined to check the answer. Thanks to the hierarchy of DNS, a scammer cannot both give false keys and false answers. The public key is part of an unbroken and trusted chain of keys, all the way up to the top level. To make DNSSEC to work, every link of the chain must be DNSSEC secured.

DNSSEC solves the problem with false answers to lookups in DNS. It is however important to be aware that DNSSEC is a small part of a big puzzle of security actions needed to make the Internet secure. DNSSEC makes sure that you come to the web address you want to reach, but does not make the content of the website you are accessing more secure.

3 DNSSEC DEPLOYMENT: CASE STUDY OF TZNIC

Tanzania Network Information Center (tzNIC) is a non-profit organization and a Public Private Partnership (PPP) established by the Tanzania Communications Regulatory Authority (TCRA) and Tanzania Internet Service Providers Association (TISPA) to manage and control the operations of the ccTLD (country code Top Level Domain) for Tanzania, .tz .

One element of tzNIC's strategic goal has been ensuring security of its services to the Internet community. To achieve this goal, tzNIC commenced the process of securing its DNS services way back in 2010 by sending its staff to various DNSSEC trainings.

It took about 2 years to achieve the goal as .tz DS record was added in the root zone in 2012. The deployment process took some time as the target was to deploy DNSSEC using self-signing platform that is scalable and sustainable.

The above deployment gave tzNIC an international mileage and did put .tz country code Top Level Domain (ccTLD) on the world map, by being the 3rd country in Africa and 100th in the world to deploy such superior security technology (DNSSEC) at its facility.

The above achievement helped tzNIC to be voted by both ISOC and ICANN as the second best registry in Africa at the 47th ICANN meeting held in Durban, South Africa in 2013.

4 RECOMMENDED DNSSEC DEPLOYMENT

Factors that EACO member states can follow for the successful deployment of DNSSEC are:

i. Management Readiness and Technical Team Readiness:

Management readiness

The will to support the project in terms of having the activity in its strategic objectives. Once the will was there then efforts to source for funding was obvious.

Technical readiness

The Technical team to have acquired enough knowledge to manage the DNS system well and ready to train for DNSSEC deployment.

Having the management will and assured funding thereafter the ball fell in the Technical Team hands and below are the issues that had to be taken into account:

ii. Capacity Building of the Technical Team

The team should be competent in DNS. Thorough understanding of the DNS is a pre-requisite to DNSSEC deployment – Don't think of deploying DNSSEC if you still have problems with DNS both theoretically and practically.

The team needs to have necessary knowledge to deploy DNSSEC. There are a number of lot of free trainings are available – NSRC, ICANN, ISOC, AfTLD, AFRINIC, et cetera.

The team needs to have the understanding of industry best practices and current RFCs;

Article I. Benchmarking with Registries that had deployed DNSSEC was also important. CZNIC was our benchmarking registry.

Article II. Current RFCs – RFC 4033 (DNS Security Introduction and Requirements), RFC 4034 (Resource Records for the DNSSEC), RFC 4035 (Protocol Modifications for the DNSSEC), RFC 4470 (Minimally Covering NSEC Records and DNSSEC On-line Signing), RFC 4642 (DNSSEC Operational Practices), RFC 5155 (DNSSEC Hashed Authenticated Denial of Existence), RFC 6014 (Cryptographic Algorithm Identifier Allocation for DNSSEC), and RFC 4398 (Storing Certificates in the Domain Name System).

iii. Infrastructure Analysis

a. Identify current infrastructure issues (both hardware and software support capabilities)
b. Optimize current DNS infrastructure to ensure it is working properly
c. Ensure all DNS operations are monitored
d. Document all the current DNS infrastructure

iv. Infrastructure Upgrade

a. Analyze the DNSSEC support capability of the current registry software
b. Analyze the current network infrastructure support capability of DNSSEC (EDNS0)
c. Analyze the DNS software support capability for DNSSEC (This includes the Master and all slave servers for your zone)

v. Set the DNSSEC Test Bed

Explore all possible DNSSEC deployment options. Almost all major DNS server software come with inbuilt DNSSEC support I.e. BIND, NSD, Unbound, Power DNS,

Knot DNS. One can opt to use these features or those of the third party software such as OpenDNSSEC and ZKT.

vi. Decide on the Best Path

a. Analyze on whether to use BIND-Tools, openDNSSEC, ZKT, etc

b. Identify the tools to use i.e. software and parameters to use on the keys generated i.e. A decision has to be made on the length of key to be used, algorithm to sign the key, how long should you keep your keys before rolling them, Time To Live etc. All these decisions have to be documented in your policy. A decision around this is usually based on the industry standards and best common practices. It may sometime depend on the registry operating environment.

c. Analyze key management options and decide based on security needs, budget availability, etc. A decision around adopting a Hardware Security Module or a Soft HSM for storing the keys is entirely based on the security levels the registry is willing to put. Some involve banks for storing the private keys and strict procedures on the personnel involved in the keys ceremony.

d. Decide the integration method of the registry software to the selected option. A careful plan of adding the signer to the zone generation life cycle is required. A basic and most used approach being Registry —-> Signer ——> Primary Server i.e. A signer receives the zone generated by the registry, signs it, checks for errors, if all is well it sends it to the primary server which in turn distributes it to all secondary servers.

vii. Develop the DNSSEC Practice Statement

DNSSEC Practice Statement (DPS) is a public document that states the practices and provisions in providing zone signing and distribution services.

viii. Actual Implementation Using the Chosen Technologies

Consider key backups, recovery sites as part of Best Current Practice (BCP).

ix. Marketing DNSSEC as a Service

Train and motivate Registrars and also promote DNS validation at ISP level.

5 Main Stages of DNSSEC Deployment

The DNSSEC Deployment can be categorized in five deployment stages as follows

i. Experimental

In this stage, the registry experiments DNSSEC in some way. The registry is identified to be in this stage primarily by doing some work with DNSSEC. Registries under this stage may be doing among the following: communicating DNSSEC related messages on various mailing lists, presentations of DNSSEC matters at conferences or events, participating at DNSSEC training workshops, issuing blog post or other online articles etc

ii. Announced

At this stage the registry makes a statement publicly committing to deploy DNSSEC and sign the Top Level Domain (TLD). This could be in the form of a news release, a blog post, a conference presentation or an email from an authoritative representative of the TLD to various DNS-related mailing lists that exist.

iii. Partial

In this stage, the registry is publicly signed with DNSSEC but the Delegation Signer (DS) record has not yet been published in the root zone of DNS. The TLD registry has gone through the work to have the authoritative name servers publish signed records, but has not yet linked the TLD into the global chain of trust.

Similar to the earlier two stages we typically learn that a TLD is in the "partial" stage by way of observing statements either online or at events. However, unlike the earlier stages, we are then able to confirm the existence of the DNSSEC signatures in the records for the TLD zone.

iv. DS in Root

When the root zone of DNS publishes a DS record for a TLD, that TLD is now tied into the "global chain of trust" of DNSSEC and second-level domains under that TLD can now have DNSSEC validation performed on them that will verify the signatures all the way back up to the DNS root.

This is the stage that one can observe and be notified when new DS records are published. The DNSSEC Statistics sites can be used to validate the status of deployment by telling when new DS records are published https://www.internetsociety.org/deploy360/dnssec/statistics/

v. Operational

The final stage of DNSSEC deployment is one in which the TLD registry is now accepting signed delegations from second-level domains, either using a DS record or a DNSKEY record depending upon the TLD policy. It is at this point that a domain registrant can now work with the Registrar and DNS hosting company to sign their domain and upload their DS record.

6 DOCUMENTATION

i. DPS document for .tz

The DPS (DNSSEC Policy and Practice Statement) document describes how the registry is securing and operating DNSSEC secured zones. The DPS document is composed in accordance with the format and contents as recommended in RFC6841. It contains descriptions of the keys, algorithms and rollover procedures used by the registry, as well as a description of the infrastructure and how the signing chain and the keys are secured. tzNIC's DPS is available at: https://tznic.or.tz/images/docs/dps-v1.1.pdf

ii. Other readings

For a detailed tutorial on DNSSEC deployment you may refer to: https://www.dns-school.org/Documentation/dnssec_howto.pdf