.zadna

ZA SLD TECHNICAL STANDARDS 2015

The purpose of this document is to outline the (a) the manner in which all ZA Second-Level Domains (SLDs) operation should be handled (b) set and define operational and the technical standards that all ZA SLDs are required to meet.

.ZA SLD GENERAL OPERATIONS STANDARDS

TABLE OF CONTENTS

1. PREAMBLE

The ZA Second Level Domain General Policy is the overarching policy of the .ZA namespace and takes precedence over all existing and future policies of ZADNA and the SLDs. Therefore, in the event where provisions of this document are found to be in conflict with the General Policy, the General Policy will take precedence.

The operation of SLD infrastructure must adhere to all related ZA policies and standards, including applicable SLD Charter and relevant RFCs that ZADNA adopts for application to the .ZA namespace.

2. TERMS AND DEFINITIONS

(Terms and Definitions in italics denote terms extracted from the Act.)

"Administrator" means the entity responsible for .ZA SLD operations and administrations duties;

"Authoritative Name Server" For purposes of this document, an Authoritative Name Server is a DNS Server that has been designated to answer authoritatively for the designated zone.

"Act" *means the Electronic Communications and Transactions Act 25 of 2002;*

"Charter" as a noun means the 'constitution' of a Second-Level Domain, specifying, inter alia, the purpose and nature of the Second-Level Domain, the criteria for registration of domain names within the Second-Level Domain, and the manner of administration of the Second-Level Domain; as a verb means the establishment of a Charter for a Second-Level Domain, which process is completed upon approval of the Charter by ZADNA;

"Domain Name" *means an alphanumeric designation that is registered or assigned to persons or entities in an SLD in respect of an electronic address or other resource on the Internet;*

"Hostname" A Hostname is the name of a DNS Server. For example, ns1.coza.net.za;

"Personal Information" as defined in the Protection of Personal Information Act 4 of 2013, means information relating to an identifiable, living natural person;

"RFC" Request for Comments (RFC) means a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet;

"Registrant" means a holder of a Domain Name;

"Registrar" means an entity that is authorised by ZADNA in terms of the Act or that is accredited by a Registry to register Domain Names and update Registry Data on behalf of Registrants in an SLD;

"Registrar Agreement" means the standard agreement to be concluded between the Registry and the Registrar in respect of a particular SLD;

"Registry" or **"Registry Operator"** means an entity authorised by ZADNA to manage and administer a specific SLD, including the provision of Primary and Secondary Name Servers and Whois Servers in relation to the relevant SLDs;

"Registry Data" means Domain Name data collected by the Registry from Registrars as part of, or following from, the registration of a Domain Name, which includes data for Registrars sponsoring registered Domain Names and Name Servers, Registrar identity, Registrar contact information, and the Registrar's administrative, billing, and technical contacts;

"Registry Database" means a database comprising of Registry Data in an SLD;

"Registry Operator" is a person to whom the custodial management and control of an SLD is delegated in terms of ZADNA's SLD Establishment and Dis-establishment Policy;

"Second-Level Domain" or "SLD" means a sub-Domain immediately following ZA, which may be unrestricted or restricted to a particular community, person or group, such as, for example, GOV.ZA (restricted) and CO.ZA (unrestricted);

"Whois" means the protocol used to provide a public information service in relation to the Registry Data;

".ZA" means South Africa's country code Top-Level Domain (ccTLD), which is delegated according to the two-letter codes in the International Standard ISO 3166-1, which is an identification label that is assigned for a particular country, and which is capable of defining a realm of administrative autonomy;

ZADNA" means the .ZA Domain Name Authority; and

"Zone Records" mean the technical resource information for each Domain Name that links each Domain Name to an IP address, and which information includes Authoritative Name Servers, start-of-authority (SOA), mail exchanger (MX) (if required by a Registry), Glue records (if necessary), and DNSSec information (if applicable), and is intended for insertion into SLD zone file;

3. BACKGROUND AND PURPOSE

3.1 Second-Level Domain

A Second-Level Domain (SLD) is a sub-domain that is immediately following a Top-Level Domain (e.g. .GOV.ZA). The .ZA country code Top-Level Domain (ccTLD) uses an SLD model, which allows for registration of Domain Names at the third-level of the Domain Name System (DNS) hierarchy.

Some .ZA SLDs are restricted and moderated (e.g. EDU.ZA, LAW.ZA and GOV.ZA), others are un-restricted and therefore un-moderated (e.g. CO.ZA, and WEB.ZA), and others are restricted but un-moderated (e.g. ORG.ZA and NET.ZA).

3.2 Purpose

The purpose of these standards is to ensure that all .ZA SLDs comply with the current best administrative and technical practices. The SLD Technical Standards set minimum technical and operation requirements that SLD Administrators/Registries must adhere to in order to become, or continue to serve as .ZA SLD Operator and Administrator.

In the event an SLD Administrator is unable to adhere to the minimum requirements set in these standards, the Administrator must notify ZADNA, and ZADNA may provide the necessary technical support to enable the Administrator to adhere to the standards. ZADNA may also assume, as an interim measure, the SLD Registry operation responsibilities for that particular SLD until a compliant Registry is appointed.

3.3 Terminology

The keywords “must” and “should” used in this document signify different types of requirements:

- **Must** signify that the defined course of action is absolutely required; and
- **Should** defines a recommended course of action that is not compelled to implement.

4. TARGET AUDIENCE

.ZA SLD Administrators and Registries must comply with the standards advocated in this document. Domain Name Registrars should familiarize themselves with the contents of this document in order for them to understand the requirements for interaction with .ZA SLD Administrator and Registries in the process of Domain Name registrations.

Failure by the SLD Administrator/Registry to comply with these Standards may lead to ZADNA, in its sole discretion, requiring the SLD administration or operation to be transferred to another SLD Administrator and/or Registry Operator.

5. TECHNICAL STANDARDS FOR ZA SLDs

5.1 Name Server compliance

Each ZA SLD must have a minimum of three (3) Authoritative Name Servers, and the hosts must not resolve to the same IP address. The number of Authoritative Name Servers should not exceed ten (10).

5.1.1 Valid Hostnames

The Hostnames used for the Name Servers must comply with the requirements for valid hostnames described in RFC 1123, section 2.1.

5.1.2 Name Server reachability

The Name Servers serving ZA SLDs must be able to answer DNS queries over either the UDP and TCP protocols on port 53 or any designated port.

User Datagram Protocol (UDP) provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet) when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

Transmission Control Protocol (TCP) provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the

sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.

5.2 Secondary Name Server location diversity compliance

Authoritative Name Servers for ZA SLDs should be placed such that that at least one Server will be available to all significant parts of the Internet in case of failure.

Authoritative Name Servers failure occurs when the specified Name Server is either unreachable or have not been correctly configured for the SLD. Authoritative Name Servers should be placed at both topologically and geographically dispersed locations on the Internet to minimize the likelihood of a single failure disabling all of them. (Refer to RFC: 2182)

5.3 DNSSec compliance

Once ZADNA finalizes its DNSSec Policy and Procedures, ZA SLD Administrators must ensure that they implement DNSSec in their zones. DNSSec is a suite of extensions that add security to the DNS protocol. The core DNSSec extensions are specified in RFCs 4033, 4034, and 4035 and add origin authority, data integrity, and authenticated denial of existence to DNS.

Suggested technical parameters for DNSSec implementation are;

- ZSK Size 1024 bits, lifetime one (1) month
- KSK size 2048 bits, lifetime one (1) year
- Zone signed with NSEC3 and Opt-Out

5.4 EPP equivalent compliance

SLDs should use EPP-equivalent Registry system or a secure method for domain management (e.g. SSL website) to interact between Registry and Registrar. Extensible Provisioning Protocol (EPP) is the standard protocol used by a majority of gTLDs and ccTLDs, particularly the Registrars and Registries in managing Domain Names (register, renew, modify, delete, transfer) and other elements in a Shared Registry System environment.

5.5 Anycast compliance

There must be at least one (1) Anycast Name Server per SLD. Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers.

5.6 Name Server software genetic diversity

RFC 2870 suggests that it is desirable to have genetic diversity in Name Server software. ZA SLD Administrators must ensure that not all Authoritative Name Servers are using the same genealogy of Name Server software. Recommended software includes BIND, NSD, Knot-DNS, and PowerDNS.

5.7 IPV6 and IPV4 compliance

SLD Administrators must ensure that respective SLD zones can answer queries using both IPV4 and IPV6 protocol. At least one Name Server must be able to answer IPV6 queries.

5.8 TSIG zone transfer compliance

SLD Administrators must ensure that transaction signature (TSIG) is used for zone transfer between Master and Slaves Servers. TSIG is a mechanism used to secure DNS messages and to provide secure Server-to-Server communication between Master and Slave Server.

5.9 Upwards referrals / recursive lookups

Authoritative Name Servers must not generate upwards referrals. A referral is a pointer to a DNS Server authoritative for a lower or upper level of the Domain Namespace. SLD Administrators responsible for Name Servers that are vulnerable to denial of service attacks, as a result of upward referrals, must reconfigure their Name Servers to not respond to upwards referrals.

RFC 2870 suggests that Authoritative Name Servers should not answer recursive requests. Recursive DNS queries occur when a DNS Client requests information from a DNS Server that is set to query subsequent DNS Servers until a definitive answer is returned to the Client. The main reason for this is to avoid the possibility of cached DNS responses polluting the

authoritative answers. For this reason, ZADNA requires that secondary Name Servers serving ZA SLDs must not answer recursive queries.

5.10 DNS monitoring

SLD Administrators must ensure that there is a mechanism for monitoring the stability of their Authoritative Name Servers and services, e.g. DNS provisioning and Whois services, which mechanism may be in the form of a monitoring software.

6. REGISTRY DATA BACKUP PROVISIONING

The Registry Operator must have a backup mechanism for their Registry Data including Whois and historical registrations, and must grant ZADNA access to such Registry Data and comply with additional Registry Data backup requirements that ZADNA may determine. ZADNA may provide its backup facility and require SLD Administrator to use the facility. Historical registration refers to the previous information that is related to particular Domain Name i.e. previous registration and/or updates of information for a particular Domain Name.

7. PERIODIC VALIDATION OF DOMAIN NAMES

The SLD Administrator must ensure that Whois data remains up to date, and that Domain Names do not become discarded. Measures of keeping Whois data up to date may be in the form of, but not limited to:

- Periodic renewal fees, where Domain Name fees are applicable;
- Technical check of the DNS information for a Domain Name; and
- Email to Registrant/Registrar confirming Whois information

8. ZA REGISTRATION STATISTICS

All Registry Operators must generate and produce monthly SLD statistics and make them available to ZADNA in the following format, or any other format ZADNA may determine from time to time:

- Total number of Domain Names in Whois (Active and inactive);
- Total number of Domain Names currently in the zone file (actively published);
- Total number of New Domains registered in the past 12 months;
- Total number of Deleted Domains in the past 12 months;
- Total number of Modified Domains in the past 12 months; and
- Total number of Validated Domains in the past 12 months.

9. WHOIS DATABASE COMPLIANCE

SLD Registry Operators must publish Whois information and it must include:

(a) The name, physical address, email address and telephone number of the Registrant in the following format:

(i) Registrant Name
(ii) Registrant Street
(iii) Registrant City
(iv) Registrant State/Province
(v) Registrant Postal Code
(vi) Registrant Country Code
(vii) Registrant Telephone Number
(viii) Registrant Email

(b) The name and contact details of the Registrar responsible for the concerned Domain Name and contact details of technical and administrative contacts for the Domain Name in the following format:

(i) Registrar Name
(ii) Registrar Street
(iii) Registrar City
(iv) Registrar State/Province
(v) Registrar Postal Code
(vi) Registrar Country Code
(vii) Registrar Telephone Number
(viii) Registrar Email

(c) If appropriate, the name and contact details of the technical, administrator or reseller responsible for the concerned Domain Name and contact details of technical and administrative contacts for the Domain Name in the following format:

(i) Registrar Name
(ii) Registrar Street
(iii) Registrar City
(iv) Registrar State/Province
(v) Registrar Postal Code
(vi) Registrar Country Code
(vii) Registrar Telephone Number
(viii) Registrar Email

(d) Zone Records associated with the registered Domain Names, including Hostnames, DNSSec and glue IP addresses as appropriate.

The Registry must ensure that personal information of Registrants is not put at risk when providing the Whois service, and must take necessary steps to protect the Whois database from un-authorized or unwarranted intrusion and data scraping. This may include limiting the number of searches a user can make in a day, and/or implementing a Captcha function to confirm that the Whois search is actually performed by a natural human being.

==========

END

Version 4 – 2015-10-13 revised for comments