1 System Description

The Domain Name Services (Pty) Ltd whois system supports both RFC 3912 port 43 whois and a web based system. The system is designed for high performance and high availability by ensuring that the system is scalable, redundant and geographically dispersed. Diagram DNS-DetailedWhoisVM.pdf provides an overview of the dotAfrica TLD initial whois service implementation

Figure 1: DNS-DetailedWhoisVM.pdf

1.1 Master Site Implementation

The hardware in use at the master site at startup phase will consist the following servers:

Port 43 whois servers

HTTP based query servers

Rate limiting servers

Query cache servers

Database servers

The master whois server cluster is replicated onto a co-hosted hot standby server cluster with incoming queries across the primary server and the standby server shared.

The system fully complies with the requirements of Specification 4 of the Registry Agreement.

1.2 Redundant Site Implementation

At the startup phase there will be a single redundant site with an identical server configuration to the primary site. Queries between the redundant site and the primary site are shared by means of an anycast address setup.

Additional geographically dispersed redundant sites will be added as whois query volume demand grows.

2 Synchronisation

Both the port 43 and the Web based whois services are considered critical infrastructure.

The whois system is replicated synchronously to the onsite standby system and is up to date to the point of the last transaction.

The whois system is replicated asynchronously to a remote standby site. Changes are replicated continuously and are well within the limits allowed by specification 10 of the registry agreement.

Geographical fail-over between the sites is achieved using any-cast IP addresses such that if one site becomes unreachable whois queries will continue un-effected.

3 Data Object Specifications

Objects returned by the whois system comply with specification 4 of the registry agreement. All data returned is in plain text format in key-value pairs. Additional formats may be provided at a later date as requested by the community or specified by ICANN.

Sample data returned by the port 43 service for the domain example.africa

_sample.txt

4 Lookups

4.1 Search Capabilities

The RFC 3912 system only allows domain name lookups. The web based whois tool is a full feature system. Two types of users are catered for:

Unauthenticated users. I.e the average anonymous Internet user.

RFC 5731:- Authenticated Registrars or nominated authenticated users.

4.1.1 Unauthenticated Users

The user may search for domain names only. Information returned is identical to as returned by the port 43 whois system other than being formatted for web browsers. Information is returned when the query exactly matches the domain.

The user may use wild card queries. Eg: examp*.africa. In this case a list of the matching domains are returned. The user may then click on the domain to view its details. To prevent data-mining abuse only a subset of the matches are returned.

4.1.2 Authenticated Users

Authenticated users have access to a full featured system offering partial match capabilities on at least the following fields:

1. Domain name
2. Registrant's name
3. All sub-fields described in EPP (e.g., street, city, state or province, contact numbers etc.)
4. Registrant and or billing, registrar or other contact ids,

Exact match search will be offered on the following:

1. Registrar id
2. EPP host objects (server names).
3. Glue records (IP addresses)

The system will allow for Boolean combinations of fields using the standard AND, OR and NOT operators.

Returned results will always include the domain names as per the specification. Objects owned by the authenticated user (e.g a registrar querying a list of their owned domains) will be fully displayed while objects owned by other registrars will honour any `<contact:disclose>` settings.

The level of information displayed for non owned objects will be adjusted from time to time as per industry and ICANN recommended best practice as determined by the dotAfrica Policy Oversight Committee

4.2 Abuse Prevention

Unauthenticated users are controlled by a rate limiting system to prevent wholesale mining of the whois database.

Authenticated users will also be limited but to a much lesser degree. All matching objects owned by the requester will be returned in a search. A

limited subset of matching objects will be returned when the objects are NOT owned by the requester.

Two aspects of abuse prevention are covered by the rate limiting system.

IP Address:- - Abuse originating from a single IP address or range of IP addresses will be limited by a Token Bucket algorithm separate to other mechanisms but having the highest priority.

Domain Name:- - Abuse on a single domain name will have an isolated limitation based on the algorithm above to prevent multiple sources querying the same name. This prevents denial of service issues when a domain name is due for deletion and multiple source continuously query the domain to check for availability.

If a user exceeds the limits imposed by the token bucket system on the web based whois system the user is then required to enter a CAPTCHA test to continue using the system.

dotAfrica undertakes to add additional measures if it becomes apparent that large amounts of information are being retrieved by any single entity.

5 RFC 3912 Compliance

The implementation conforms with the requirements of RFC 3912 (WHOIS Protocol Specification)

A whois query to the system connects to TCP port 43 on the public WHOIS server. A single domain name is sent with the line terminated by a carriage return and a new line. The server responds with the result of the whois query in plain ASCII.

Since RFC 3912 does not specify any details for internationalisation, the whois service of the dotAfrica TLD will provide ASCII character set data. This implies that where EPP contact addresses exist of both local and international types, the International version will be returned.

RFC 5733 disclosure settings are honoured when returning information.

For example

```
<contact:disclose flag="0">
    <contact:email/>
    <contact:voice/>
</contact:disclose>
```

will prevent the registrant's email or contact number from being displayed in the whois query.

6 Resourcing Requirements

The dotAfrica TLD development, deployment and operational responsibilities for the above will be staffed by members of the ZA Central Registry during start-up phase. Once the dotAfrica TLD becomes operational dedicated staff will initially be deployed to manage both the RFC 3912 whois and the web based whois as follows

Technical Manager:- - 1 staff member responsible for all technical related issues including keeping up to date with international standards and best practises.

System Administration:- - 2 staff members responsible for the day to day system administration and system monitoring.

7 Bulk Access

Bulk access here is defined as a full copy of the whois database.

Bulk access of objects in the Whois service will only be provided to ICANN or their appointed agents in accordance with the specifications 4 and 10 of the ICANN Registry Agreement.