1 Synopsis

This chapter provides details on the ZA Central Registry Shared Registry System Extensible Provisioning Protocol EPP functionality as will be used by the dotAfrica TLD.

2 Overview

The functionality of the ZA Central Registry Shared Registry System allows registrars to interface using the EPP protocol and commands as defined in the following RFCs and as referenced in this document:

RFC 3735:- Guidelines for Extending the EPP.

RFC 5730:- EPP Description.

RFC 5731:- EPP Domain Name Mapping.

RFC 5732:- EPP Host Mapping.

RFC 5733:- EPP Contact Mapping.

RFC 5734:- EPP TCP Transport.

RFC 5910:- EPP DNSSEC.

The ZA Central Registry Shared Registry System also conforms to the above-mentioned RFCs.
The ZA Central Registry does not provide support for Domain Registry Grace Period Mapping as per RFC 3915.
The ZA Central Registry will not be supporting International Domain Names at startup.

3 Registrar Interface

The dotAfrica implementation listens for incoming TCP connection requests. Once a client has issued an EPP `<login>` command on the listening port, the server responds, creating the required session and sending back an EPP `<greeting>` to the client.

To end a session, a client may close the connection by issuing EPP `<logout>` command or an active close call.

The dotAfrica implementation automatically closes a session once the session has idled for 24 hours.

A total of 2 concurrent sessions per client are allowed.

A Registrar can only establish a TCP connection to the server if they have been technically accredited, provided the ZA Central Registry with their public key and the public key has been successfully installed.

Exchanging of messages between client and server conforms to the requirements outlined in RFC 5734, and follows the general client-server message exchange as outlined in **Figure 1** of RFC 5734 Section 3.

Pipelining commands is possible. The server supports command pipelining to a maximum limit of the connection buffer of 16384 bytes.

The dotAfrica implementation returns a message from the server to the client for every command performed. If a message is lost due to connection failure, the result code can only be retrieved if the client issues the same command using the same client transaction identifier `<clTRID>` .

The dotAfrica implementation uses SSL/TLS as well as IP based Access Control Lists. A session is started on login only if an SSL handshake is established and the client IP Address is listed on the Access Control List. Further security measures include authentication through use of usernames and passwords. A session is terminated upon logout. A session is valid for 24 hours.

The dotAfrica handling and interpretation of the EPP Data Units conforms to RFC 5734 Section 4, whereby the format of any EPP data unit will contain the 32-bit header describing the total length of the data unit, and the EPP XML Instance.

Length and calculation of data units conform with requirements outlined in RFC 5734 .

Changes in the implementation can be made and will have to be decided by the dotAfrica Policy Oversight Committee .

4 Extensible Provisioning Protocol (EPP)

This section describes the capability of the ZA Central Registry Shared Registry System EPP and compliance with RFC 5730

4.1 Protocol Description

EPP is an XML based protocol used for provisioning domains and their associated objects. The dotAfrica EPP implementation supports all commands

as defined in RFC 5730.

4.2 Protocol Commands

A command is any action performed on an object. Commands are grouped into session, query and object transformation commands as follows in the list below:

Protocol:-

- login
- logout

Query:-

- Check
- Info
- Poll
- Transfer

Transform:-

- Create
- Delete
- Renew
- Transfer
- Update

4.3 EPP `<login>` Protocol Command

The dotAfrica implementation of the EPP `<login>` command conforms to the requirements outlined in RFC 5730 Section 2.9.1.1.

4.4 EPP `<logout>` Protocol Command

The dotAfrica implementation of the EPP `<logout>` command conforms to the requirements outlined in RFC 5730 Section 2.9.1.2 .

4.5 EPP `<poll>` Protocol Command

The dotAfrica implementation of the EPP `<poll>` command conforms to the requirements outlined in RFC 5730 Section 2.9.2.3 .

4.6 Command Response

For each EPP command that is issued by the client to the server, a corresponding response will be returned to the client by the server.

Every response will contain a result code. The result code indicates command success or failure. The dotAfrica implementation conforms to the theory of result codes outlined in RFC 5321 Section 4.2.1 and uses a fourth digit in its response codes.

5 EPP Domain Name Mapping

5.1 Overview

The following section provides details on how the ZA Central Registry Shared Registry System maps its domain functionality. Any changes to the EPP Domain Name Mapping command set will be determined by the dotAfrica Policy Oversight Committee .

5.2 Relationship of Domain Objects and Host Objects

All created domain name objects require a minimum of 2 unique subordinate or delegated host objects.

5.3 Object Attributes

Domain and Host Names:- Only domain names conforming to standard ASCII will be used. Internationalized Domain Names (IDN)s must be provided in A-Label format.

Contact and Client Identifiers:- Client and contact identifiers will be represented through a clID element to create an association with a domain object.

Status Values:- The dotAfrica implementation supports server and client status interaction outlined in RFC 5731.

Dates and Times:- All dates and times conform to RFC 5731 and are represented using UTC.

Validity Periods:- The dotAfrica implementation supports validity periods in months and years, as well as a combination of both.

Authorisation Information:- The dotAfrica implementation supports domain name object authorisation through use of passwords as defined in RFC 5731. Passwords are stored in one-way hash format.

5.4 EPP `<check>` Command

The dotAfrica implementation of the EPP `<check>` command conforms to the requirements outlined in RFC 5731 . The Domain `<check>` command will be limited to 100 checks per command.

5.5 EPP `<info>` Command

The dotAfrica implementation of the EPP `<info>` command conforms to the requirements outlined in RFC 5731 Section 3.1.2. The `<info>` command response will be restricted based on the requester credentials. Expiry dates and other information will not be presented to unauthorized sources.

5.6 EPP `<transfer>` Command

The dotAfrica implementation of the EPP `<transfer>` command conforms to the requirements outlined in RFC 5731.

The dotAfrica implementation supports the following EPP `<transfer>` operations which conform to RFC 5730 :

"query":- Allows a client to identify the current status of a transfer request on a domain name object.

"request":- Allows a client to request a transfer of a domain object from one sponsor to another.

"cancel":- Allows a client to cancel their transfer request for a domain as long as the domain has not yet been transferred.

"approve":- Allows the current domain sponsor to approve a transfer request for the requested domain.

"reject":- Allows the current domain sponsor the reject a transfer request for the requested domain.

The dotAfrica implementation incorporates an e-mail voting system whereby a registrant is allowed to vote on the transfer of a domain. An EPP Poll message will be queued for the current sponsor for transfer vote notification.

5.7 EPP <create> Command

The dotAfrica implementation of the EPP <create> command restricts the use of the <period> element where the registry defines the registration period of a domain object.

5.8 EPP <delete> Command

The dotAfrica implementation of the EPP <delete> command conforms to the requirements outlined in RFC 5731 Section 3.2.2 . The dotAfrica implementation denotes that any domain that undergoes a <delete> command is checked to conform to subordinate host dependencies outlined in RFC 5731 . A deletion request on a domain object will be prohibited if the subordinate host objects are referenced by other domains belonging to the same registrar.

5.9 EPP <renew> Command

The dotAfrica implementation of the EPP <renew> command restricts the use of the <domain:period> element. The domain object can only be renewed to a maximum of one period.

5.10 EPP <update> Command

The dotAfrica implementation of the EPP <update> command conforms to the requirements outlined in RFC 5731 . The dotAfrica implementation utilises the <domain:contact> element to set "tech", "billing", "admin" contacts to domain name objects.

6 EPP Host Mapping

The following section provides details on how the ZA Central Registry Shared Registry System maps its host functionality. The dotAfrica implementation restricts the host creation and usage to the individual registrar. In other words each registrar controls and maintains their own set of hosts even if the names are duplicated with other registrars. Subordinate host glue publication is strictly controlled to prevent nameserver masquerading.

6.1 Relationship of Domain Objects and Host Objects

All created domain name objects require a minimum of 2 unique subordinate or delegated host objects.

6.2 Object Attributes

Host Names:- Only host names conforming to standard ASCII will be used.

Status Values:- The dotAfrica implementation supports server and client status interaction outlined in RFC 5732.

Dates and Times:- All dates and times conform to RFC 5732 and are represented using UTC.

Glue:- The dotAfrica implementation supports IPv4 and IPv6 addresses, conforming to the requirements outlined in RFC 0791 and RFC 4291 respectively.

6.3 EPP `<check>` Command

The dotAfrica implementation of the EPP `<check>` command conforms to the requirements outlined in RFC 5732 .

6.4 EPP `<info>` Command

The dotAfrica implementation of the EPP `<info>` command conforms to the requirements outlined in RFC 5732 .

6.5 EPP `<create>` Command

The dotAfrica implementation of the EPP `<create>` command conforms to the requirements outlined in RFC 5732. The use of the Host create command might be restricted in lieu of the Domain Host handling during Domain update and creation. The eventual Host create usage will be determined by the dotAfrica Policy Oversight Committee .

6.6 EPP `<delete>` Command

The dotAfrica Implementation of the EPP `<delete>` command conforms to the requirements outlined in RFC 5732.

The dotAfrica implementation denotes that any host that undergoes a `<delete>` command is checked for dependencies outlined in RFC 5731 .

6.7 EPP `<update>` Command

The dotAfrica implementation of the EPP `<update>` command conforms to the requirements outlined in RFC 5732.
The dotAfricaimplementation dictates that the changing of a host object information is performed through the domain object mapping using the domain `<update>` command.

7 EPP Contact Mapping

7.1 Overview

The following section provides details on how the ZA Central Registry Shared Registry System maps its contact functionality.
Any changes to the EPP Contact Mapping command set will be determined by the dotAfrica Policy Oversight Committee . In the dotAfrica implementation the Registrar objects are stored as standard EPP Contact objects, thus allowing a registrar to adjust contact information such as passwords or support addresses.

7.2 Object Attributes

Contact and Client Identifiers:- Client and contact identifiers will be represented through a clID element to create an association with a domain object.

Status Values:- The dotAfrica implementation supports server and client statuses outlined in RFC 5733. Status combination interactions conform to RFC 5733 .

Internationalized Postal Info:- The dotAfrica implementation supports postal information represented as a subset of UTF-8 encoding in 7-bit ASCII. All required and optional elements for a contact object are supported by the dotAfrica implementation.

Localized Postal Info:- The dotAfrica implementation also supports postal information represented in UTF-8 encoding. All required and optional elements for a contact object are supported by the dotAfrica implementation.

Telephone Numbers:- The dotAfrica implementation conforms to RFC 5733 by ensuring that all telephone numbers begin with a plus ("+") sign followed by a country code as defined in ITU.E164.2005, followed by a dot ("."), followed by a sequence of digits representing the telephone number.

E-mail Addresses:- The dotAfrica implementation conforms to the requirements for e-mail addresses as defined in RFC 5322.

Dates and Times:- All dates and times conform to RFC 5733. The dotAfrica implementation supports time zone representation in UTC format.

Authorisation Information:- The dotAfrica implementation supports contact object authorisation through use of passwords, conforming to outlined requirements in RFC 5733. Passwords are stored in one-way hash format.

Disclosure of Contact Elements and Attributes:- The dotAfrica implementation supports disclosure of contact attributes and conforms to RFC 5730, by announcing its data collection policies. The dotAfrica implementation supports the disclosure elements outlined in RFC 5733.

7.3 EPP `<check>` Command

The dotAfrica implementation of the EPP `<check>` command conforms to the requirements outlined in RFC 5733 .

7.4 EPP `<info>` Command

The dotAfrica implementation of the EPP `<info>` command conforms to the requirements outlined in RFC 5733. The disclosure of Contact information will obey the disclose options as provided for the Contact object.

7.5 EPP `<transfer>` Command

The dotAfrica implementation of the EPP `<transfer>` query command conforms to the requirements outlined in RFC 5733.

7.6 EPP `<create>` Command

The dotAfrica implementation of the EPP `<create>` command conforms to the requirements outlined in RFC 5733 .
The dotAfrica implementation supports the creation of a contact object with

both <contact:postalInfo> types of "loc" and "int", conforming to the requirements outlined in RFC 5733 Section 3.2.1 .

7.7 EPP <delete> Command

Implementation of the EPP <delete> command conforms to the requirements outlined in RFC 5733 Section 3.2.2.

Current policy states that a contact object cannot be deleted if in any way it is associated with another object. If a contact object is still associated with a domain object, the contact object is not deleted until the association between contact and domain objects is removed.

7.8 EPP <update> Command

The dotAfrica implementation of the EPP <update> command conforms to the requirements outlined in RFC 5733 .
The dotAfrica implementation supports the updating of a contact object with both <contact:postalInfo> types of "loc" and "int", conforming to the requirements outlined in RFC 5733 Section 3.2.5 .

8 EPP Technical Plan

The Technical Layout will include the following:

- On-site Scalable Master Server with the following configuration:

  Message Server:- The Message Server is responsible for handling session management, access control, user authentication EPP schema validation and Poll commands.

  Registry Engine:- The Registry Engine is responsible for all object level query and transform commands.

  Database:- The primary Registry Engine database.

- Scalable Standby Co-located Server with the following configuration:

  Message Server:- A secondary Message Server used in the event that the Master Server fails.

Registry Engine:- A secondary registry Engine used in the event that the Master Server fails.

Standby Database:- A secondary database that is used in the event that the primary database on the Master Server fails.

- Off-site Remote Standby Server with the following configuration:

  The Remote Off-Site Server configuration is a mirror of the Master site.

From the Technical Layout above, the EPP Technical Plan is as follows:

The initial startup of the EPP System involves starting the Master server as well as a Standby server. The Standby server acts as a failover measure in the event that the Master server fails.

EPP traffic is received via the External Network Bus, flows to the Message Server. The Message Server handles all access control, SSL session management, authentication and EPP schema validation in accordance to RFC 5731 to 5733 and RFC 5910. The Registry Engine handles authentication of Registrars as well as processes all EPP commands in accordance with RFC 5730.

The Standby Server acts as a failover server in event that the Master Server fails. The Standby server is in a constant waiting state and is monitored for availability in the event that is needs to be used. In the event that the Master Server is overloaded, the Standby Server may be used for load balancing.

The Remote Standby System is an off-site server that is a complete duplication of the Master Server and the Standby Server. In the event that the Master Server and Standby Server fail, the Remote System will act as a failover and perform exactly as the Master and Standby Servers.

The Remote Off-Site Server will be located at the Johannesburg Internet Exchange (JINX). Both the primary site (hosting the Master Server and Standby Co-Located Server) and the backup site (hosting the Remote Off-Site Server) are highly redundant, state of the art data centers with multiple power supplies, on-site backup facilities, and offer protection from natural disasters.

Scalability for the EPP System covers hardware scalability related to system utilization. Additional servers and required hardware will be added for the Master Server as well as the Standby Co-Located Server as resource utilization nears 50%. Any scalability changes made to the Master Server and Secondary Co-Located server will also be duplicated to the Remote Off-Site Server.

9 DNSSEC

The dotAfrica implementation supports the DNSSEC and conforms to RFC 5910. The ZA Central Registry will be operating as a thick registry. A thick registry reflects on DNSSEC in the following way:

Only DNSKEYS will be supported. The Registry will generate the corresponding DS record.

The provided DS record is used for validation purposes only.

Removal of DS records will not be supported on the client side.

Removal of DNSKEYS will remove the associated DS record.

Any changes to the DNSSEC EPP Command Mapping will be determined by the dotAfrica Policy Oversight Committee .

10 EPP Resourcing

The following section provides a high level description of the related infrastructure, human and system resources as provided by the ZA Central Registry and as will be utilised and expanded on for the dotAfrica TLD.

10.1 SRS Human Resource

The ZA Central Registry has a compliment of 6 RE administrators, developers, testers and support staff responsible for the development and day to day operational requirements including the following roles

System Testing:- Responsibility covers regression testing for all new releases, as well as providing Registrar documentation and notices regarding any issues that may crop up from time to time.

System Administration:- Responsibility covers administration of the RE including installation, configuration, and operating system installation and configuration.

System Monitoring:- Responsibility covers monitoring of the hardware dedicated to the RE, RE uptime, RE performance, security and abuse monitoring, and general operating system health.

Backups:- Responsibility covers the backup requirements of the RE machines including total system backup and log backups.

Development and Maintenance:- Responsibility covers the development and maintenance of the RE system including registry policy updates as may be required from time to time as registry policy changes dictate, SRS performance monitoring, reporting, statistics gathering, etc.

10.2 Registrar Technical Support

The ZA Central Registry uses its human resources to provide technical support to Registrars beyond the day to day operational requirements, including:

Registry Online Portal:- Support covers the development and maintenance of the online Registry portal, updating EPP related frequently asked questions and the EPP Command wiki pages.

Registrar Technical Assistance:- The Registry portal incorporates an online contact mechanism where a Registrar can electronically ask a question and acquire technical support relating to their enquiry. Enquiries are tracked through a ticketing system, offering a platform for effectively monitoring and tracking Registrar enquiries.

Accreditation Support:- The ZA Central Registry offers online capability for Registrars to follow a policy aligned process for acquiring accreditation. The accreditation process is performed in 6 steps as listed below:

1. Providing Registrar contact information
2. Providing Company Registration Document
3. Providing contact information for a primary contact
4. Providing additional information including Registrar logo
5. Reviewing status of integration with the EPP system
6. Uploading of SLL Certificate and acquiring live system credentials

Support relating to accreditation comes in the form of answering accreditation process related queries, assigning test account credentials to newly applied Registrars, monitoring accreditation progress and providing live account credentials for accredited Registrars.

Key Management Support covers the safe acquisition of SSL Certificates from accredited Registrars. Accredited Registrars can safely request to change their current in-use key.

Any alterations to or removal of proprietary extensions will be determined by the dotAfrica Policy Oversight Committee .

11 Domain Extensions

The following section provides the domain name proprietary extensions implemented by the ZA Central Registry for the dotAfrica TLD. All proprietary extensions conform to the requirements outlined in RFC 3735, and are written in RFC format as below.