dotAfrica gTLD DNSSEC Policy Statement

ZA Central Registry

April 7, 2014

Contents

1 Acknowledgments

2 Introduction

This document provides the dotAfrica gTLD statement of security practices and provisions that are applied in conjunction with DNSSEC in the dotAfrica top-level domain. This document conforms with the Draft IETF Standard
draft-ietf-dnsop-dnssec-dps-framework-05 - DNSSEC Policy & Practice Statement Framework. The DPS is one of several documents relevant to the operation of the dotAfrica gTLD.

2.1 Overview

DNSSEC is a set of records and protocol modifications that enable the authentication of DNS data and also make it possible to ensure that content has not been modified during transfer, including mechanisms for authenticated denial of existence. Resource records secured with DNSSEC are cryptographically signed and incorporate asymmetric cryptography in the DNS hierarchy, whereby trust follows the same chain as the DNS tree, meaning that trust originates from the root and is delegated in the same way as the ownership of a domain. The following IETF RFCs are referenced in this document:

RFC 1034

RFC 1035

RFC 4033

RFC 4034

RFC 4035

RFC 4509

RFC 4641

RFC 5155

RFC 5702

RFC 5910

2.2 Document name and identification

Document title: dotAfrica-DNSSEC-Policy.pdf
Version: 0.4
Created: 19 January 2012
Updated: 15 March 2012

2.3 Community and Applicability

The following roles and delegation of liability have been identified.

2.3.1 Registry

dotAfrica bears responsibility for the Internet's Africatop-level dotAfrica domain. dotAfrica administrates domain names that identify underlying zones in the dotAfrica zone. This means that dotAfrica manages supplements, changes and removal of all data that is related to a domain name. The Registry is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys. The Registry is also responsible for securely signing all authoritative DNS resource records in the dotAfrica zone. The Registry is also responsible for generating delegation signer DS records based on provided DNSKEY records for each domain. Finally, the Registry is responsible for the secure export and publication of trust anchors TA and the registration and maintenance of delegation signer DS resource records in the root zone.

2.3.2 Registrars

A Registrar is the party that is responsible for the administration and management of domain names of behalf of the Registrant. The Registrar handles the registration, maintenance and management of a Registrants domain name and is an accredited dotAfrica partner. The Registrar is responsible for securely identifying the Registrant of a domain. The Registrar is responsible for adding, removing or updating specified DNSKEY records for each domain at the request of the Registrant.

2.3.3 Registrants

A Registrant is the physical or legal entity that controls a domain name. Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DNSKEY records through the Registrar.

The Registrant is responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

2.3.4 Relying Party

The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate TAs. The relying party must also stay informed of any relevant DNSSEC related events in the dotAfrica domain.

2.3.5 Applicability

Each Registrant is responsible for determining the relevant level of security for their domain. This DPS is exclusively applicable to the top-level dotAfrica domain and describes the procedures and security controls and practices applicable when managing and employing keys and signatures for dotAfrica's signing of the dotAfrica zone. With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the dotAfrica domain and assess their own risk.

2.4 Specification Administration

This DPS is updated as appropriate, such as in the event of significant modifications in system or procedures that affect the content of the document.

2.4.1 Specification administration organization

Domain Name Services Pty Ltd

2.4.2 Contact Information

Address: CoZa House, Corporate Park South, Midrand, South Africa
Tel: +27.113140077
Fax: +27.113140088
URL: http://www.registry.net.za
e-mail: info@dnservices.co.za

2.4.3 Specification change procedures

Amendments to this DPS are either made in the form of amendments to the existing document or the publication of a new version of the document. This DPS and amendments to it are published at `http://registry.africa` Only the most recent version of this DPS is applicable. dotAfrica reserves the right to amend the DPS without notification for amendments that are not designated as significant. It is in the sole discretion of the specification administrator to designate changes as significant, in which case dotAfrica will provide notice. Any changes will be approved by the specification administrator and may be effective immediately upon publication.

3 Publication and Repositories

3.1 Repositories

dotAfrica publishes DNSSEC relevant information on dotAfrica's website at `http://registry.africa`.

The electronic version of this DPS at this specific address is the official version.

Notifications relevant to DNSSEC in dotAfrica will be distributed by e-mail.

3.2 Publication of Key Signing Keys (KSK)

dotAfrica will publish KSKs in the form of a DNSKEY and DS as follows:

1. dotAfrica's website, `http://registry.africa`
2. Directly in the root zone (only DS)

3.3 Access controls on repositories

Information published at the specific website is available to the general public and is protected against unauthorized adding, deletion or modification of the content on the website.

4 Operational Requirements

4.1 Meaning of domain names

A domain name is a unique identifier, which is often associated with services such as web hosting or e-mail, as defined by RFC 1034 and RFC 1035. Certain trademark and copyright restrictions may apply to the new registration of domain names in the dotAfrica Registry

4.2 Activation of DNSSEC for child zone

DNSSEC is activated by a DNSKEY record for the zone being sent from the Registrar to the Registry and a DS record being generated and published in the DNS, which established a chain of trust to the child zone. The Registry will perform a reverse check against the provided name-servers to verify that the provided record matches the child zone key. The Registry will also perform a validation check against any DS records provided with the request.

4.3 Identification and authentication of child zone manager

It is the responsibility of the Registrar to securely identify and authenticate the Registrant through a suitable mechanism, and in compliance with the stipulations in the contract between dotAfrica and the Registrar.

4.4 Registration of delegation signer (DS) resource records

The Registry accepts DNSKEY records through the EPP interface from each Registrar. The DS record is then generated through the process indicated in RFC 4509. The DNSKEY record must be valid and sent in the format indicated in RFC 5910 (EPP DNS Security Extensions Mapping).

4.5 Method to prove possession of private key

The Registry does not conduct any controls with the aim of validating the Registrant as the manager of a private key. The Registrar is responsible for conducting the controls that are required and those deemed necessary.

4.6 Removal of DS record

A DNSKEY record is deregistered by issuing the relevant EPP DNSSEC update command. The deregistration of the DNSKEY record will deactivate the DNSSEC security mechanism for the zone in question.

4.6.1 Who can request removal

Only the Registrant, or the party formally designated by the Registrant by assigning the Registrar role, has the authority to request deregistration of the DS records.

4.6.2 Procedure for removal request

The Registrant or the Registrant's representative tasks the Registrar with implementing the deregistration. The Registrar may only do this on behalf of the Registrant. From the time the deregistration request has been received by dotAfrica via EPP, it takes no longer than until the next zone generation for the change to be recorded in the zone file. Subsequently, it takes the TTL (1 hour) plus the distribution time before the changes have been deployed. The whole procedure may take a maximum of 2 hours to complete.

4.6.3 Emergency removal request

If a Registrant finds himself in a situation in which he is unable to reach the Registrar, dotAfrica can deregister the DNSKEY record, provided that is it possible to securely identify the Registrant via password based authentication and biometric (passport/ID document).

5 Facility, Management and Operational Controls

5.1 Physical Controls

dotAfrica has implemented physical security controls to meet the requirements specified in this DPS.

5.1.1 Site location and construction

dotAfrica will establish two fully operational and geographically dispersed operation centers, at least 5 kilometers apart. The redundant facility will contain a complete set of the Registry's critical systems, whose information

will be continuously updated through automatic replication of the normal operations facility. All of the systems components will be protected within a physical perimeter with an access control and alarm system operated by dotAfrica. The backup operations facility meets the minimum standards applied to the normal facility in terms of physical security, power supply, environment, and fire/water protection.

5.1.2 Physical access

Physical access to the protected environment will be limited to authorized personnel. Physical access is restricted by biometric based access control, stored passwords, and key cards. Entry is logged and the environment will be continuously monitored. Online HSMs are protected by locked cabinets and offline HSMs will be protected through the use of locked safes.

5.1.3 Power and air conditioning

In the event of power outages, power will be provided by UPS until the backup power systems have begun to generate electricity. The backup power systems will have the capacity to supply critical resources with electricity.

5.1.4 Water exposures

The facilities will implement flooding protection and detection mechanisms.

5.1.5 Fire prevention and protection

The facilities will be equipped with fire detection and extinguishing systems. The facilities will be equipped with automatic extinguishers with dry extinguishing, fireproof floors and each room constitutes an independent fire cell.

5.1.6 Media storage

The Registry's guidelines for information classification define the requirements imposed for the storage of sensitive data.

5.1.7 Waste disposal

Disposed storage media and other material that may contain sensitive information will be destroyed in a secure manner, either by the Registry or by a contracted party.

5.1.8 Off-site backup

Certain critical data will also be securely stored using a third-party storage facility. Physical access to the storage facility will be limited to authorized personnel. The storage facility will be geographically and administratively separated from dotAfrica's other facilities.

5.2 Procedural Controls

5.2.1 Trusted roles

Trusted roles are held by persons that are able to affect the zone file's content, delivery of trust anchors or the generation or use of private keys. The trusted roles are:

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

5.2.2 Number of persons required per task

At any given time, there must be at least two individuals within the organization per trusted role indicated in 5.2.1.
Key generation requires two people to be present; one from each role.
The export and control of trust anchors requires two people to be present; one from each role.
None of the aforementioned operations may be performed in the presence of unauthorized people.

5.2.3 Identification and authentication for each role

Only people who have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with the Registry may hold a trusted role. Before a person receives their credentials for system access, a valid form of identification must be presented. Refer to 5.3.2.

5.2.4 Tasks requiring separation of duties

The trusted roles in 5.2.1 above may not be held simultaneously by one and the same person.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must be able to present proof of the requisite background and qualifications.

5.3.2 Background check procedures

The evaluation of background checks is conducted by the HR function at dotAfrica. The control of backgrounds and qualifications includes reviewing

- The candidate's resume
- Previous employments
- References (unclassified and others)
- Documentation confirming the relevant and completed education
- Financial position through a credit check
- Criminal background check

To qualify for any of the trusted roles, the controls cannot reveal any discrepancies that indicate unsuitability.

5.3.3 Training requirements

The Registry provides the relevant and requisite training regarding procedures, administration and the technical systems that are associated with each trusted role. Tests are carried out after each completed training course and the results are registered in the person's skills logbook.

The training courses include:

- dotAfrica's operations (equivalent to the certification training program for Registrars).
- The role's scope, areas of responsibility and authority.
- General domain-name administration.
- Basic technical proficiency in DNS and DNSSEC (for Security officers SO)

- Advanced technical proficiency in DNS and DNSSEC (for System Administrators SA)
- Basic knowledge of information security.
- Administration, procedures and checklists.
- Procedures for incident management.
- Procedures for crisis management.

5.3.4 Retraining frequency and requirements

People holding trusted roles must participate in new tests and possible supplementary training courses every third year and in the event of major changes.

5.3.5 Job rotation frequency and sequence

The responsibility for conducting operations is rotated on each occasion between the people who hold a trusted role.

5.3.6 Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are regulated in the responsibility agreement. Severe negligence may lead to termination and damage liability.

5.3.7 Contracting personnel requirements

In certain circumstances, dotAfrica may need to use contractors as a supplement to full-time employees. The contractors wll sign the same type of responsibility agreements as full-time employees. Contractors who have not been subject to a background check and training, and thus are not qualified for a trusted role, may not participate in the activities indicated in 5.2.2.

5.3.8 Documentation supplied to personnel

dotAfrica Registry and IT operations supply the documentation necessary for the individual employee to perform their work task in a secure and satisfactory manner.

5.4 Audit Logging Procedures

Logging is automatically carried out and involves the continuous collection of information regarding the activities that take place in an IT system. The logged information is used in the monitoring of operations, for statistical purposes and for investigation purposes in suspected cases of violation of dotAfrica's policies and regulations. Logging information also includes the journals, checklists and other paper documents that are vital to security and that are required for auditing. The purpose of the collected log information is to be able to reconstruct the case after-the-fact and analyze which people or applications/systems did what and at what time. Logging and the identification of users enables such features as traceability and the follow-up of unauthorized use.

5.4.1 Types of events recorded

The following events are included in logging:

- All types of activities that involve Key Management, such as key generation, key activation, and signing and exporting keys.
- Remote access, successful and unsuccessful.
- Privileged operations.
- Entry to a facility.
- Database Transactions and changes
- EPP Command messages

5.4.2 Frequency of processing log

Logs are continuously analyzed through automated and manual controls. Specific controls are conducted on processes including key generation, system reboots and detected anomalies.

5.4.3 Retention period for audit log information

Log information is stored in log systems for not less than 30 days. Thereafter, the log information is archived for not less than 5 years. Database table audit logs will persevere indefinitely.

5.4.4 Protection of audit log

All electronic log information is stored at all operations facilities at the same time. The logging system is protected against unauthorized viewing and the manipulation of information.

5.4.5 Audit log backup procedures

All electronic log information is securely backed up on a nightly basis and is stored separately from the system in a secure location.

5.4.6 Audit collection system

Electronic log information is transferred in real-time to the collection systems; one for each facility and external to the key generating system.

5.4.7 Notification to event-causing subject

The personnel concerned are informed that logging is taking place. The personnel are not entitled to request to view log data.

5.4.8 Vulnerability assessments

All anomalies in the log information are investigated to analyze potential vulnerabilities.

5.5 Compromise and Disaster Recovery

5.5.1 Incident and compromise handling procedures

All real and perceived events of a security-critical nature that caused or could have caused an outage or damage to the IT system, disruptions and defects due to incorrect information, or security breaches are defined as incidents. All incidents are handled in accordance with the Registry's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, what effects the incident has had or may have had, measures to prevent the incident from recurring and forms to further report this information. An incident that involves suspicion that a private key has been compromised leads to the immediate rollover of keys pursuant to the procedures indicated in 5.5.3.

5.5.2 Corrupted computing resources, software, and/or data

In the event of corruption, the incident management procedures shall be initiated and appropriate measures shall be taken.

5.5.3 Entity private key compromise procedures

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:

- If a Zone Signing Key (ZSK) is suspected of having been compromised, it will immediately be removed from production and stopped being used. If necessary, a new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or timed out. If a ZSK is suspected of having been compromised is revealed to unauthorized parties, this will be notified through the channels indicated in 3.1.
- If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents. A KSK rollover in progress is always notified through the channels indicated in 3.1.
- If a KSK is lost, a new key will be generated with new DS record. A request to IANA to publish the additional DS corresponding to the new KSK will be issued. Once IANA changes are propagated, the old DNSKEY is taken out of service and swapped for the new DNSKEY. At such time, the change is announced using the mechanisms defined in 3.1. During the time preceding the rollover, the key set remains static and any scheduled ZSK rollover is postponed until the KSK swap is complete.

5.5.4 Business Continuity and IT Disaster Recovery Capabilities

The Registry has a contingency plan that ensures that operation-critical production can be relocated between the two operation facilities within four hours. The facilities are equivalent in terms of physical and logistical protection. Information is replicated in real-time between the facilities. Frequently used spare components and critical hardware components are stored onsite in each operations facility. The contingency plan and routines are regularly

tested. The completed tests and trials are recorded and subsequently evaluated. The contingency plan includes:

- Who decides on the activation of a emergency recovery procedures.
- How and where the crisis management shall convene.
- Activation of backup operations.
- Appointment of a Task Manager.
- Criteria for restoring normal operations.

5.6 Entity termination

If the Registry must discontinue DNSSEC for the dotAfrica zone for any reason and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed. If operations are to be transferred to another party, the Registry will participate in the transition so as to make it as smooth as possible.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Key generation takes place in a hardware security module HSM that is managed by trained and specifically appointed personnel in trusted roles. Key generation takes place when necessary and must be performed by two people working in unison. The necessary 2 people are present during the entire operation. The entire key-generation procedure is logged, part of which is done electronically and part of which is done manually on paper by the SO.

6.1.2 Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SO and SA. The SO is responsible for publishing the public component of the KSK in a secure manner as per 3.1. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

6.1.3 Public key parameters generation and quality checking

Key parameters are regulated by dotAfrica's KASP (Key and Signing Policy) and quality control includes checking the key length.

6.1.4 Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system. A signature that is created by a DNSSEC key for either a ZSK or a KSK never has a longer validity period of more than eight days (six days plus two days of jitter), and this validity period always begins when the temporary signature has been established.

6.2 Private key protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed in the hardware module and no private keys are ever found unprotected outside HSM.

6.2.1 Cryptographic module standards and controls

The system uses a hardware security module HSM which conforms to the requirements in FIPS 140-2 level 3.

6.2.2 Private key (m-of-n) multi-person control

The Registry does not apply multi-person controls for HSM activation. An SO is required to activate the module, which in turn requires physical access, which can only be performed by the SA.

6.2.3 Private key escrow

The Registry does not apply a key escrow.

6.2.4 Private key backup

The key archive is encrypted with a Storage Master Key SMK. The master key is stored on a portable storage medium in a bank vault, which can only be accessed by an SO. Keys are stored in an encrypted format on the signing module's hard drive. The encrypted key archive is securely backed up and synchronized between the operations facilities on a daily basis or immediately following a key generation.

6.2.5 Private key storage on cryptographic module

The Storage Master Key SMK is shared by all security modules in the system. The master key is used to decrypt the key archive that is stored outside the security module while deactivated.

6.2.6 Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

6.2.7 Private key transfer into or from a cryptographic module

During the installation of the signing system, a joint HSM key (or Storage Master Key, SMK) is transferred via a portable USB media, after which the HSM is locked to prevent further export of keys. The USB media is subsequently stored in accordance with 6.2.4

6.2.8 Method of activating private key

Private keys are activated by unlocking the HSM. An SA provides an SO with access to the facility. The SO states a personal passphrase for the HSM through a console.

6.2.9 Method of deactivating private key

The HSM is locked if the signing system is either turned off or rebooted.

6.2.10 Method of destroying private key

Private keys are not destroyed. After their useful life, they are removed from the signing system.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Public keys are archived in accordance with the archiving of other information relevant to traceability in the system, such as log data.

6.3.2 Key usage periods

Keys become invalid as they are taken out of production. Old keys are not reused.

6.4 Activation data

The activation data is the personal passphrase for each SO that is used to activate the HSM.

6.4.1 Activation data generation and installation

Each SO is responsible for creating their own activation data pursuant to the applicable requirements of at least nine characters of varying nature.

6.4.2 Activation data protection

Each SO is responsible for protecting their activation data in the best possible way. On the suspicion of compromised activation data, the SO must immediately change it.

6.4.3 Other aspects of activation data

In the event of an emergency, there is a sealed and tamper evident envelope in a secure location that contains activation information with instructions on appointing an Emergency Security Officer (ESO). dotAfrica's DNSSEC contingency plan procedures state the conditions in which this shall be applied.

6.5 Computer Security Controls

All critical components of the Registry's systems are placed in the organizations secure facilities in accordance with 5.1. Access to the server's operating systems is limited to individuals that require this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

6.6 Network Security Controls

The Registry has logically sectioned networks that are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. All sensitive information that is transferred over the communications network is always protected by strong encryption.

6.7 Timestamping

The Registry retrieves time that is traceable to timeservers from `africa.pool.ntp.org`. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

6.8 Life Cycle Technical Controls

6.8.1 System development controls

All source code is stored in a version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe. dotAfrica's development model is based on industry standards and includes:

- Fully functional specification and documented security requirements,
- Documented architectural design based on a natural modularization of the system,
- Continuous pursuit of minimizing complexity,
- Systematic and automated testing and regression tests,
- Issuing of distinct software versions,
- Issuing Version Control Tags upon release
- Constant quality follow-ups of detected defects.
- Constant reliability follow-ups
- Post-delivery maintenance

6.8.2 Security management controls

Authorization registers are kept and followed up regularly. The Registry also conducts regular security audits of the system. The Registry prepares and maintains a system security plan that is based on recurring risk analysis.

6.8.3 Life cycle security controls

The Registry complies with ITIL Change Management.

7 Zone Signing

7.1 Key lengths and algorithms

Key lengths and algorithms are to be of sufficient length for their designated purpose during each key's useful life. Algorithms shall be standardized by the IETF, available to the public and resource efficient for all parties involved. The RSA algorithm with a key length of 2048 bits are currently used for KSK and 1024 bits for ZSK.

7.2 Authenticated denial of existence

The Registry uses NSEC3 records as specified by RFC 5155, and may sort zones prior to signing, in order to maximize NSEC3 efficiency.

7.3 Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA2 (RSASHA256, RFC 5702).

7.4 Zone signing key roll-over

ZSK rollover is carried out every 28th day with a pre/post period of 7 days either side for new/old keys respectively.

7.5 Key signing key roll-over

KSK rollover is carried out every 730th day with a pre/post period of 30 days either side for new/old keys respectively.

7.6 Signature life-time and re-signing frequency

RR sets are signed with ZSKs with a validity period of between six and eight days. Resigning takes place every other odd UTC hour.

7.7 Verification of Zone Signing Key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. The abovementioned is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the dotAfrica Start Of Authority (SOA).

7.8 Verification of resource records

The Registry verifies that all resource records are valid in accordance with the current standards prior to distribution.

7.9 Resource records time-to-live

Controlled using the dotAfrica, Key And Signing Policy (KASP. (DNSKEY = 3,600 seconds. SOA = 85,706 seconds. RRSIG inherits TTL from the RR set that it signs.

8 Compliance Audit

Audited documents (policy, procedures, requirements), information regarding facts or other information that is relevant in consideration of the audit criteria and that is verifiable are used as documentation when conducting audits.

8.1 Frequency of entity compliance audit

The need of audits is decided by dotAfrica. Circumstances which may entail an audit requirement are:

- Recurring anomalies.
- Significant changes that are made at the management level, in the organization or in processes.
- Other circumstances, such as the competence among personnel, new equipment or other major changes.

8.2 Identity/qualifications of auditor

The auditor shall be able to demonstrate proficiency in IT security, DNS and DNSSEC.

8.3 Auditor's relationship to audited party

An external auditing manager shall be appointed for the audit. When necessary, the auditing manager shall be able to recruit specific expert knowledge. The auditing manager is responsible for implementation during the entire audit.

8.4 Topics covered by audit

The auditing manager's assignment includes ensuring that:

- The right competence represents dotAfrica.
- The auditee is informed and prepared prior to the audit.
- The auditee is informed of the topic of the audit in advance.
- Follow-up procedures of the audit results are in place.

8.5 Actions taken as a result of deficiency

The auditing manager shall immediately verbally inform dotAfrica's management of any anomalies.

8.6 Communication of results

The auditing manager shall submit a written report of the audit results to dotAfrica not later than 30 calendar days after the audit.

9 Legal Matters

9.1 Fees

dotAfrica Registry may impose administrative fees for DNSSEC from Registrars. The fees shall be decided upon by the policy oversight committee.

9.2 Privacy of personal information

9.2.1 Responsibility to Protect Personal Information

Regulated by dotAfrica's Registration terms and conditions and by agreement between the Registry and the Registrar.

9.2.2 Disclosure of Personal Information to Judicial Authorities

Decisions regarding the disclosure of personal information to judicial authorities may be made upon direct request. The matter of disclosure is decided case-by-case. Decisions are made by dotAfrica's legal department.

9.3 Limitations of liability

Liability of damage between the Registry and the Registrar is regulated by the Registrar agreement. dotAfrica's liability of damage toward Registrants is regulated by the Registration terms and conditions that are applicable to the top-level dotAfrica domain.

9.4 Term and termination

9.4.1 Validity Period

This DPS applies until further notice.

9.4.2 Expiration of Validity

This DPS does not expire but can be replaced by newer versions.

9.4.3 Dispute Resolution

Any dispute or conflict resulting from this Agreement shall be filed at any South African Court.

9.4.4 Governing Law

Africa Union AU defined rules and regulations shall apply to this DPS.