	INFORMATION SECURITY POLICY
	ISSUE SPECIFIC POLICY
	VERSION: VI09 2018-12-14
	EFFECTIVE DATE: 2018-12-14

LAWtrust Root Certification Practice Statement (LAWtrust Root CA 2048)

Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07

("LAWtrust")

85 Regency Drive,

Route 21 Corporate Park, Irene, Centurion,

Pretoria, South Africa

Phone +27 (0)12 676 9240 • Fax +27 (0)12 665 3997

Web https://www.lawtrust.co.za • eMail governance@lawtrust.co.za

LAWtrust reserves the right to change or amend this certification practice statement at any time without prior notice. Changes will be posted on the LAWtrust website [https://www.lawtrust.co.za/repository] from time to time. If you have any queries about this document, please contact LAWtrust.

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V1.0 01-11-2011	01/11/2011	Niel van Greunen	Initial version prepared for Microsoft Root submission	Expired
V2.0 01-05-2012	01/05/2012	Niel van Greunen	Review before Root CA key ceremony	Expired
V3.0 01-11-2012	01/11/2012	Niel van Greunen	Changes after the 2012 KPMG SANS21188/WebTrust audit	Expired
V4.0 10-12-2013	01/04/2014	Niel van Greunen	Review and minor editorial changes, added LAWtrust Subordinate CA key archival	Expired
V5.0 18-11-2015	01/12/2015	Bruce Anderson	Review and change location where Root CA server is stored to bio-vault at hosted data centre	Expired
V006 2016-12-21	2016-12-21	Bruce Anderson	Amended logo Added approval Signature on last page	Expired
V007 2017-02-21	2017-02-21	Bruce Anderson	Changes including Housekeeping items from 2016	Expired
V008 2017-10-16	2017-10-16	Bruce Anderson	2017 Review	Expired
VI009 2018-12-14	2018-12-14	Eduard Oosthuizen	Apply new document template, 2018 Review	Operational

Document references

References to the following documents have been made in the preparation of this document:

Ref.	Document Title	File Location
1	LAWtrust Certificate Policy	LAWtrust Internal Policy (Level 2)
2	LAWtrust AeSign CEN-SSCD RA Charter	https://www.lawtrust.co.za/repository
3	LAWtrust Relying Party Agreement	https://www.lawtrust.co.za/repository
4	LAWtrust Subscriber Agreement	https://www.lawtrust.co.za/repository
5	LAWtrust Privacy Policy	https://www.lawtrust.co.za/pages/privacy-notice
6	LAWtrust mPKI Services Agreements	LAWtrust & Registration Authorities

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

This document is the Certification Practice Statement (CPS) of the following Root Certification Authorities managed by LAWtrust:

1. LAWtrust Root Certification Authority 2048 (LAWtrust Root CA 2048);

The LAWtrust Root CA 2048 CPS describes the certification practices that have been implemented to ensure the LAWtrust Root CA's trustworthiness in signing sub ordinate CA certificates. It has been drafted to satisfy the requirements of the LAWtrust Certificate Policy (CP) for issuing LAWtrust Subordinate CA Certificates.

The LAWtrust Root CA 2048 CPS is intended to allow participants to the LAWtrust public key infrastructure (PKI) to assess the trustworthiness of the LAWtrust Root CA 2048 and determine suitability of LAWtrust Subordinate CA Certificates in meeting the requirements in the communication of electronic information.

1.2 Document name and identification

This document title is "LAWtrust Root Certification Practice Statement (LAWtrust Root CA 2048 CPS)". You may consider the version of the LAWtrust Root CA 2048 CPS available for download from the LAWtrust website [https://www.lawtrust.co.za/repository] as the most current and authoritative version as at the time of downloading.

1.3 PKI participants

1.3.1 LAWtrust Root CA 2048

The LAWtrust Root CA 2048 is the trust anchor for all subordinate CAs (i.e. Issuing CAs) that operate under this CPS.

This offers certificates with the following hierarchies

LAWtrust Root Certification Authority 2048 (Root CA)

- LAWtrust Certification Authority (Issuing CA)
  - Subscriber

The Issuing CAs that operate under the provisions of this CPS are established as part of the Key Ceremony Process. This process is a witnessed process whereby the Issuing CAs keys are generated and the public key signed by the Root CA.

1.3.2 LAWtrust Issuing Certification Authorities

LAWtrust is the legal Entity which owns the Issuing Certificate Authorities whose certificates are issued by the LAWtrust Root CA. LAWtrust is responsible for all Information Security, management, operational and Business Continuity of all its Certification Authorities.

The LAWtrust Root CA and any issuing CA's signed by the Root CA as listed below are collectively referred to as the **LAWtrust PKI**.

LAWtrust Root Certification Authority 2048 (Root CA)

- LAWtrust AeSign CA1
- LAWtrust AeSign CA2

1.3.3 Registration authorities

The LAWtrust Operations Authority performs the role of the Registration Authority for the Root and Issuing CA's issued by the Root.

1.3.3.1 LAWtrust RA

The LAWtrust Registration Authority is a function responsible for the following functions:

- Accepting CA requests from the Policy Authority
- Validating requests from the Policy Authority

- Scheduling and implementation of the Issuing CA request once validated.

1.3.3.2 Appointed Registration Authorities

LAWtrust does not use external Registration Authorities to perform any tasks relating to the issuance of Issuing CA Certificates.

1.3.4 Relying Parties

A Relying Party is an entity that receives any LAWtrust issued digital certificate and who acts in reliance on that certificate.

1.3.5 Other participants

Other participants are entities on whom LAWtrust may rely in verifying information relating to an Applicant for issuing a LAWtrust Subordinate CA Certificate.

1.4 Certificate usage

The LAWtrust Root CA 2048 is capable of manufacturing LAWtrust Subordinate CA Certificates.

1.4.1 Prohibited certificate uses

Any use falling outside the certificate uses described in the LAWtrust Root CA 2048 CPS shall be deemed to be a prohibited use.

LAWtrust Subordinate CA Certificates are not designed or intended for use in or in conjunction with hazardous activities or uses requiring failsafe performance and the use of the certificates in this regard is strictly prohibited.

1.4.2 Appropriate certificate uses

LAWtrust Subordinate CA Certificates may be used for the following purposes:

- Signing certificate requests
- Validating LAWtrust Subordinate CA Certificates issued by the LAWtrust Subordinate CA's;

- Validating Certificate Revocation Lists issued by the LAWtrust Subordinate CA's;

1.5 Policy administration

1.5.1 Security Management

Governed by the LAWtrust Information Security Management Program, LAWtrust has structured the Policy documentation in the following manner:

Information Security Polices (Including the specific policies as stipulated in the LAWtrust Information Security Policy)

Certificate Authority Specific Polices (Including Certificate Policy, Certificate Practice Statements, Registration Authority Charters (applicable to LAWtrust Subordinate CA RA's)

1.5.2 Roles and responsibilities

In order to ensure universal adoption of the Policies LAWtrust has set up two authority bodies comprising of senior management membership. The LAWtrust Policy Authority (LAWtrust PA) shall be responsible for all Policy administration; such policies include the LAWtrust CP. The LAWtrust Operating Authority (LAWtrust OA) is the body responsible for the CPS operational implementation, this includes all procedures and standards required to ensure correct implementation of the CPS. The CPS is based on the policies established by the LAWtrust PA.

1.5.3 Organisation administering the document

The LAWtrust PA shall administer all the policies and practices relating to the LAWtrust Subordinate CA Certificate Authorities, this includes the LAWtrust CP, CPS's and LAWtrust RA Charters. The LAWtrust OA shall be responsible for the implementation of the CPS and related procedures.

1.5.4 Policy change procedures

The LAWtrust PA may, in its discretion, modify the LAWtrust Root CA 2048 CPS and the terms and conditions contained herein from time to time.

1.5.4.1 Low impact modifications

Modifications to the LAWtrust Root CA 2048 CPS that, in the judgment of the LAWtrust PA, will have little or no impact on Applicants, Subscribers, and Relying Parties, may be made with no change to the LAWtrust Root CA 2048 CPS version number and no notification to Applicants, Subscribers, and Relying Parties. Such changes shall become effective immediately upon publication in the LAWtrust Repository.

1.5.4.2 High Impact modifications

Modifications to the LAWtrust Root CA 2048 CPS that, in the judgment of the LAWtrust PA may have a high impact on Applicants, Subscribers, and Relying Parties, shall be categorised as significant changes and published in the LAWtrust Repository and shall become effective thirty (30) days after notification of such changes.

1.5.4.2.1 Definition of significant impact modifications

Modifications which are considered to have high impact include the following

1. Changes to the reliance limit of the certificates

2. Changes in encryption key generation, storage or usage

1.5.4.2.2 Version Control

In the event that the LAWtrust PA makes significant modifications to LAWtrust Root CA 2048 CPS, the version number of the LAWtrust Root CA 2048 CPS shall be updated accordingly.

1.5.5 Person determining CPS suitability for the policy

The LAWtrust PA shall determine suitability of the CPS for the LAWtrust Subordinate CA Certificate Policy.

1.5.6 Publication and notification policies

Prior to any significant changes to this LAWtrust Root CA 2048 CPS, as described in 1.5.4, notification of the upcoming changes will be posted in the LAWtrust Repository.

1.5.7 CPS approval procedures

The LAWtrust Root CA 2048 CPS is developed by the LAWtrust PA and the LAWtrust OA and approved by the LAWtrust Security Committee.

Prior to any significant changes to this CPS, as described in 1.5.4,

LAWtrust shall provide the following notification

1. South African Accreditation Authority notification will be in writing;
2. Registration Authorities will be notified via email
3. PKI Participant notification will be posted in the LAWtrust Repository.

1.5.8 Contact detail

The contact information for questions to the LAWtrust PA and LAWtrust OA is:
85 Regency Drive,
Route 21 Corporate Park, Irene,
Centurion,
South Africa
Phone +27 (0)12 676 9240
Fax +27 (0)12 665 3997
https://www.lawtrust.co.za
eMail: governance@lawtrust.co.za (PA) or mpkiops@lawtrust.co.za (OA)

1.6 Definitions

Term	Definition
applicant	An Entity making an application for a digital certificate.
Asymmetric cryptography	Asymmetric cryptography or public Key cryptography is cryptography in which a pair of keys issued to a subscriber and the keys are used to encrypt and or decrypt messages to achieve authenticity and confidentiality. An applicant applies for a digital certificate, if successful a key pair is generated and a certificate signing request is sent to a certificate Authority which then signs the public key and returns a public key certificate to the applicant. The public key and its corresponding private key are uniquely linked mathematically.
audit trail files	Secured audit log/trail files are stored on the CA server and can only be viewed by authorised personnel logged into the administration interface.
Authentication	Authentication is a mechanism to validate the identity of a user and or a computing device requesting permission to access computing resources or technology services supporting business processes.
Authentication factors	A factor of authentication refers to a mechanism used to facilitate the authentication of a user or devices requesting access to computing resources. The following factors of authentication are universally accepted; Location of the computing interface(controlled access and managed), Something the requester has(Possession of something which is validated), Something the requester knows(secret password or PIN), Something the requester is(biometrics)

Term	Definition
Authentication scheme	Industry accepted authentication schemes include one or more factors of authentication. The choice of authentication factors and the process behind establishing credentials within each factors within the chosen scheme determine the strength of the authentication.
CA	See definition of certificate/certification authority.
certificate administrator	A trusted individual that performs certain trusted tasks (e.g. authentication) on behalf of a CA or RA. This person is usually a member of the personnel of such CA or RA.
certificate	See definition of digital certificate.
certificate/certification authority	A legal Entity that issues, signs, manages, revokes and renews digital certificates.
certificate policy	A named set of rules that indicate the applicability of a digital certificate to a particular community and or class of application with common security requirements. The practices required to give effect to the rules set out in the certificate policy are set out in the certification practice statement.

Term	Definition
certification practice statement	In order to comply with the rules set out in the certificate policy, the CPS details the practices that a certificate authority needs to employ when issuing, managing, revoking, renewing, and providing access to digital certificates, and further includes the terms and conditions under which the certificate authority makes such services available.
CP	See definition of certificate policy.
CPS	See definition of certification practice statement.
Chained	A Certificate Chain linking the chain of trust from the highest level of trust, that being the Root CA, any LAWtrust Subordinate CA's and or Issuing CA's.
cryptography	Cryptography is about message secrecy, and is a main component in information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, not usually the existence of such messages.
cryptography services	A service provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of a digital certificate/digital signature scheme for the purpose of ensuring (i) that data or data messages can be accessed or can be put into an intelligible form only by certain persons, (ii) that the authenticity or integrity of such data or data message is capable of being ascertained,

Term	Definition
	(iii) the integrity of the data or data message, or (iv) that the source of the data or data message can be correctly ascertained.
data	Electronic representations of information in any form.
data message	Data generated, sent, received or stored by electronic means.
digital certificate	A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number.
digital signature	A transformation of a data message using an asymmetric cryptosystem such that a person having the initial data message and the signer's public key can determine whether: (i) the transformation was created using the private key that corresponds to the subscriber's public key; and (ii) the message has been altered since the transformation was made.

Term	Definition
digital signature validation	In conjunction with the public key component of the correct public/private key pair, the signature of a data object can be verified by: 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.
digitally sign	The act of generating a digital signature for a data message, which is created by: 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.
ECT Act 2002	See definition of Electronic Communications and Transaction Act 2002
electronic communication	Communication by means of data messages.
Electronic Communication and Transactions Act, No. 25 of 2002	South African Legislation that provides for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy; to promote universal access to

Term	Definition
	electronic communications and transactions and the use of electronic transactions by businesses.
email	Electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication.
End Entity	certificate subject that uses its private key for purposes other than signing certificates
Entity	A legal Entity or an individual or end Entity are all examples of entities. Note that a Certification Authority, a Registration Authority or an End Entity are entities.
hosted data centre	The LAWtrust hosted data centre is the facility at Vodacom.
Identity document	An identity document is used to verify aspects of a person's identity. Recognised identity documents are; For South African citizens, 1. a valid "Green" Identity document or Passport issued by the South African Home Affairs department 2. A valid South African Driver's license For non-South African Nationals, 1. a valid Passport issued by the persons country of origin Home Affairs department.

Term	Definition
integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
interoperation	In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.
key pair	Two mathematically related cryptographic keys, referred to as a private key and a public key, having the properties that (i) one key (the public key) can encrypt a message which only the other key (the private key) can decrypt, and (ii) even knowing the one key (the public key), it is computationally infeasible to discover the other key (the private key).
LAWtrust Root CA	See also the definition of certification authority. The Root certification authorities managed by LAWtrust including the LAWtrust Root Certification Authority 2048 and the LAWtrust Root Certification Authority 2 (4096)
LAWtrust Subordinate CA Certificate	See definition of digital certificate. Digital certificates issued by a LAWtrust Root CA.
LAWtrust OA	LAWtrust Management forum responsible for the implementation of the LAWtrust Policy and Practices and the Operations of the LAWtrust PKI environment

Term	Definition
LAWtrust PA	LAWtrust Management forum responsible for defining the LAWtrust Policy and Practices and ensuring that the Policies and Practices are adhered to.
LAWtrust PKI	The LAWtrust PKI includes the Root CA and all CA's established and signed by the LAWtrust Root CA.
LDAP	A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Master Services Agreement	The contract between LAWtrust and an appointed registration authority stipulating the terms and conditions for the registration authority to manage certificate lifecycle activities on behalf of the LAWtrust Root CA.
MSA	Master Services Agreement,
non-repudiation	The ability to prevent a party from refusing to fulfil an obligation or denying the truth or validity of an electronic communication facilitated by appropriate use of the LAWtrust Services.
OCSP	Online Certificate Status Protocol is an Internet protocol, employed to ascertain the revocation status of an X.509 digital certificate. An alternative to CRL based checking.

Term	Definition
OCSP Responder	An online service hosted by Lawtrust and connected to Lawtrust repositories in order to process OCSP certificate revocation checks.
private key	The key of a key pair used to create a digital signature and is required to be kept secret.
public key	The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed.
Public key cryptography	Public key cryptography is about using mathematically related keys, a public key and a private key, in order to implement a digital certificate /digital signature scheme, also known as an asymmetric crypto system.
PKI	See definition of public key infrastructure.
public key infrastructure	The structure of hardware, software, people, processes and policies that collectively support the implementation and operation of a certificate-based public key cryptography scheme.
RA	See definition of registration authority.

Term	Definition
registration authority	An Entity that: (i) receives certificate applications, and (ii) validates information supplied in support of a certificate application, (iii) requests a certificate authority to issue a certificate containing the information as validated by the registration authority, and (iv) requests a certificate authority to revoke certificates issued;
Relying Party	A person that relies on a certificate or other data that has been digitally signed.
relying party agreement	An agreement between the certificate authority and a relying party that sets out the terms and conditions governing reliance upon a certificate or data that has been digitally signed
Security Committee SC	The Security Committee is appointed by the LAWtrust CEO with responsibilities to manage, monitor and controls the implementation of information security as a whole within LAWtrust.
signature	Any mark made by a person that evidence's that person's intention to bind himself/herself to the contents of a document to which that mark has been appended. Depending on the circumstances, this could be a handwritten signature or a digital signature.

Term	Definition
subscriber	an applicant whose Certificate Application has been approved, and has been issued a certificate, and who is the subject named or otherwise identified in the certificate, controls the private key that corresponds to the public key listed in that certificate, and is the individual to whom digitally signed data messages verified by reference to such certificate are to be attributed.
Verification	Verification is the act of checking that information is accurate. It is used in the following manor a) At registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity; b) During use, the act of comparing electronically submitted identity and credentials with stored values to prove identity. c) Relying Party will check the certificates used as per the relying Party Agreement.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The LAWtrust PA maintains the LAWtrust repositories to allow access to LAWtrust Subordinate CA Certificate Authority related information. The repositories host general CA documentation, certificate status information and any further information which may from time to time be required by the LAWtrust PA. There are two categories of repositories;

2.1.1 Document repository

The document repository hosts the policies and general CA documentation. Examples of the documents found in this repository include:

- The LAWtrust Root CA 2048 CPS,
- Information and agreements relating to the subscription for and reliance on LAWtrust Subordinate CA Certificates;
- The LAWtrust Root CA 2048 public certificate;
- And any further information which may from time to time be required by the LAWtrust PA.

The information in the document repository is accessible through a web-interface [https://www.lawtrust.co.za/repository] and is periodically updated in terms of the LAWtrust Root CA 2048 CPS.

2.1.2 Certificate status repository

The LAWtrust Subordinate CA's Certificate statuses are published in the following format;

- CRL1 (web interface access):

  The LAWtrust Root CA 2048 Certificate Revocation List (CRL's) is accessible through the web-interface:

[http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl]

and is periodically updated in terms of the LAWtrust Root CA 2048 CPS.

Online Certificate Status Protocol are not specified as a validation mechanism for the LAWtrust Root CA 2048.

2.2 Publication of the LAWtrust Root CA 2048 CPS

The LAWtrust Root CA 2048 CPS is available from LAWtrust in hardcopy upon request. This LAWtrust Root CA 2048 CPS, published in the LAWtrust repository, shall be available by web-interface [https://www.lawtrust.co.za/repository] at all times subject to any interruption of the LAWtrust website services.

Changes or modifications to this LAWtrust Root CA 2048 CPS shall be published in accordance with directions given by the LAWtrust PA as documented in section 1.5.4.

2.2.1 Time or frequency of CPS publication

After acceptance by the LAWtrust PA the LAWtrust Root CA 2048 CPS shall be published in the manner described in 2.2.

The LAWtrust Root CA 2048 CPS shall be reviewed as may be required due to:

- Changes in existing practice, the introduction of new practices, changes in legislation or regulation governing the use of digital certificates or electronic signatures; or
- Changes in the PKI within which the LAWtrust Root CA 2048 provide certificates.
- Annual Review of the LAWtrust Root CA 2048 CPS.

Changes shall be documented in revised versions of the LAWtrust Root CA 2048 CPS and become effective on the dates indicated in the revised CPS.

2.3 Access controls on repositories

The LAWtrust Root CA 2048 CPS and all other documents published in the LAWtrust Repository will be available to all PKI Participants, but may only be modified by the LAWtrust PA. The LAWtrust PA will digitally sign CA related documents published in the repository to protect the document integrity.

3. IDENTIFICATION AND AUTHENTICATION

Before issuing a LAWtrust Subordinate CA Certificate the LAWtrust OA will verify the information, purpose and/or attributes of the Certificate details to be published in a LAWtrust Subordinate CA Certificate. This section of the CPS establishes the criteria for an acceptable request for a LAWtrust Subordinate CA Certificate.

3.1 Naming

3.1.1 Types of names

A LAWtrust Subordinate CA Certificate shall include a common name component as required in the X501 Standard. The common name shall be the name associated with LAWtrust.

3.1.2 Need for names to be meaningful

3.1.2.1 Naming for Entity Certificates used in the Issuing CA's:

The value of the common name attribute used in naming entity certificates is the name, in the case of any entity that requires registration, under which the entity is registered and, in the case of an entity not requiring registration, the name under which the entity conducts its activities.

3.1.3 LAWtrust Subordinate CA Rules for interpreting various name forms

In the provision of LAWtrust Subordinate CA certificates, the CA names and other attributes in the certificate distinguished name of the LAWtrust Subordinate CA will provide a unique name.

3.1.4 Uniqueness of names

The combination of the common name and other company specific attributes contained in the Distinguished Name (DN), together with the serial number attributed to the certificate provides a unique electronic identity for the LAWtrust Subordinate CA associated with the certificate. LAWtrust shall not re-use a serial number in respect of a LAWtrust Subordinate CA Certificate.

3.1.5 Name claim dispute resolution

The common names in LAWtrust Subordinate CA Certificates are issued to ensure no duplication of common names.

3.1.6 Recognition, authentication, and role of trademarks

The LAWtrust Root CA 2048 may use registered trademarks when assigning the distinguished names to LAWtrust Subordinate CA's.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

LAWtrust maintain the trust and possession of the PKI encryption keys in a scripted and witnessed process. The Key Ceremony scripts are testament to LAWtrust possession of the Private Key. Verification of LAWtrust Subordinate CA information

The LAWtrust OA shall verify the information required in the LAWtrust Subordinate CA certificate required by parties depending on the use of the LAWtrust Subordinate CA certificate.

3.2.2 Criteria for interoperation

Suitability and criteria for interoperation will be jointly determined by the LAWtrust PA and the LAWtrust OA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The LAWtrust OA shall establish proof of the LAWtrust Subordinate CA's identity and verify the accuracy of information to be published in a LAWtrust Subordinate CA Certificate subject to a routine re-key. The stringency of the verification of information shall be commensurate with the minimum stipulations of the LAWtrust PA for the LAWtrust Subordinate CA certification required.

3.3.2 Identification and authentication for re-key after revocation

The LAWtrust Root CA 2048 shall not renew or re-issue LAWtrust Subordinate CA Certificates that have been permanently revoked.

If LAWtrust wishes to use a LAWtrust Subordinate CA Certificate after revocation, the OA must request a new LAWtrust Subordinate CA Certificate to replace the LAWtrust Subordinate CA Certificate that has been revoked.

On revocation of a LAWtrust Subordinate CA Certificate LAWtrust shall immediate cease using such a LAWtrust Subordinate CA Certificate and remove the LAWtrust Subordinate CA Certificate from any devices and/or software under its direct control in which it has been installed.

3.4 Identification and authentication for revocation request

The LAWtrust OA shall authenticate the identity of a LAWtrust Subordinate CA requesting revocation of its certificate via the LAWtrust Subordinate CA web fingerprint.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

LAWtrust will perform the certificate lifecycle operations and management for all LAWtrust Subordinate CA's according to the processes specified in the LAWtrust Subordinate CA CPS's.

4.1 Certificate request

4.1.1 Who can submit a certificate request

The LAWtrust PA may submit a LAWtrust Subordinate CA certificate request to the LAWtrust OA.

The LAWtrust Root CA 2048 shall, under the LAWtrust Root CA 2048 CPS, issue:

LAWtrust Subordinate CA Certificates.

4.1.2 Subordinate CA enrolment process and responsibilities

LAWtrust PA shall:

- Complete and submit to the LAWtrust OA a request for a LAWtrust Subordinate CA Certificate providing all information requested, without any errors, misrepresentations or omissions;

LAWtrust OA shall:

On receipt of a complete request, the LAWtrust OA shall process the request and verify the information provided in terms of 3.2.

If the request or information provided to the LAWtrust OA is deficient, the LAWtrust OA shall, at its discretion:

- Notify the LAWtrust PA of the deficiency and of the refusal of the request.

If the verification of the information submitted to the LAWtrust OA is successful, then

- The LAWtrust OA shall schedule a key ceremony at the LAWtrust vault in the hosting facilities to establish the LAWtrust Subordinate CA;
- Submit, during the key ceremony, a CSR from the LAWtrust Subordinate CA to the LAWtrust Root CA 2048;
- Provide the LAWtrust Subordinate CA Certificate to the LAWtrust PA and prepare for installation.

4.2 Certificate request processing

4.2.1 Performing identification and authentication functions

The LAWtrust Root CA 2048 shall process a request for the issue of a LAWtrust Subordinate CA Certificate only after the LAWtrust OA has performed the verification checks on the information provided in the request.

Once the verification process has been completed the LAWtrust OA shall retain all relevant information in conformance with the requirements of the LAWtrust PA for a period of seven years after the expiry or revocation of the LAWtrust Subordinate CA Certificate.

4.2.2 Approval or rejection of certificate requests

This is an internal process to LAWtrust.

4.2.3 Time to process certificate requests

Any request for a LAWtrust Subordinate CA Certificate should be processed within the time deemed appropriate by the LAWtrust PA. The LAWtrust Root CA 2048 will process a CSR during a key ceremony immediately on receiving such a request from the LAWtrust Subordinate CA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The LAWtrust Root CA 2048 can only accept certificate issuance requests from the LAWtrust OA and during formal key ceremonies for LAWtrust Subordinate CA's. After

satisfying itself that the information provided to it by the LAWtrust Subordinate CA is accurate and that the verification checks required by the LAWtrust PA and performed by the LAWtrust OA have been executed, the LAWtrust Root CA 2048 may generate and digitally sign the LAWtrust Subordinate CA Certificate requested in accordance with the certificate profile described in 7.1 of the LAWtrust Root CA 2048 CPS.

4.3.2 Notification of issuance of certificate

This is an internal process to LAWtrust.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

LAWtrust shall check that the content of the LAWtrust Subordinate CA Certificate is correct.

If the LAWtrust OA is notified of any inaccuracies in the LAWtrust Subordinate CA Certificate, the LAWtrust Subordinate CA Certificate shall be revoked in terms of the provisions of 4.9 of the LAWtrust Root CA 2048 CPS.

4.4.2 Publication of the certificate by the Root CA

Post issuance the certificate is published in the appropriate LAWtrust Subordinate CA LDAP directory and in the LAWtrust Repository. (https://www.lawtrust.co.za/pages/repository).

4.4.3 Notification of certificate issuance by the Root CA to other entities

There are no further communications to other entities.

4.5 Key pair and certificate usage

4.5.1 Financial limitations on certificate usage

Not applicable.

4.5.2 Issuing CA private key and certificate usage

LAWtrust shall only use the private key associated with the LAWtrust Subordinate CA Certificate after the issue of the certificate and shall not use the private key associated with the certificate after the revocation or expiry of the LAWtrust Subordinate CA Certificate.

LAWtrust shall use its private key and the LAWtrust Subordinate CA Certificate in strict compliance with the LAWtrust Root CA 2048 CPS.

4.5.3 Relying Party public key and certificate usage

Relying Parties shall comply strictly with the provisions of the Relying Party Agreement and shall be responsible for checking the status of any LAWtrust Subordinate CA Certificate before relying on the certificate.

4.6 Certificate renewal

LAWtrust Subordinate CA Certificates may be renewed as required by business operational requirements. This is an internal process to the LAWtrust PKI.

4.7 Certificate re-key

LAWtrust Subordinate CA Certificates may be renewed as required by business operational requirements. This is an internal process to the LAWtrust PKI.

4.8 Certificate modification

The LAWtrust Root CA 2048 shall not modify LAWtrust Subordinate CA Certificates.

4.9 Certificate revocation and suspension

The LAWtrust Root CA 2048 shall revoke a LAWtrust Subordinate CA Certificate after receiving a valid revocation request from the LAWtrust OA.

LAWtrust shall be entitled to request revocation of and shall request revocation of LAWtrust Subordinate CA Certificates, if LAWtrust acquires knowledge of or has a reasonable basis for believing that any of the following events has occurred:

- The compromise of the LAWtrust Root CA 2048 private key;
- Any change in the information contained in the LAWtrust Subordinate CA Certificate;
- A determination by LAWtrust that the LAWtrust Subordinate CA Certificate was not issued in accordance with the LAWtrust Root CA 2048 CPS; or
- Any other reason that LAWtrust reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust Subordinate CA Certificate.

4.9.1 Circumstances for revocation

LAWtrust shall request revocation of a LAWtrust Subordinate CA Certificate if LAWtrust has a suspicion or knowledge of a compromise of LAWtrust's private key or that the information contained in LAWtrust Subordinate CA Certificate has become inaccurate, incomplete, or misleading as a result of change in circumstances relating to LAWtrust.

A request for revocation by LAWtrust shall be submitted to the LAWtrust OA and processed according to the processes defined in the LAWtrust Root CA 2048 CPS.

Revocation of a LAWtrust Subordinate CA Certificate shall not affect any of LAWtrust's contractual obligations under the LAWtrust Root CA 2048 CPS or any Relying Party Agreements.

4.9.2 Who can request revocation

LAWtrust may request revocation of its LAWtrust Subordinate CA Certificate at any time and for any reason.

The LAWtrust Security Committee or LAWtrust OA may request revocation of a LAWtrust Subordinate CA Certificate if it reasonably believes that the LAWtrust Subordinate CA Certificate or private key associated with the LAWtrust Subordinate CA Certificate has been compromised.

4.9.3 Procedure for revocation request

The LAWtrust OA shall authenticate a request for revocation of its LAWtrust Subordinate CA Certificate by requiring:

- A sub-set of the information provided by LAWtrust with LAWtrust Subordinate CA Certificate request; or
- The CSR submitted by LAWtrust with LAWtrust Subordinate CA Certificate request; or
- Verification of the web fingerprint for the LAWtrust Subordinate CA under which the LAWtrust Subordinate CA Certificate has been issued.

On receipt of confirmation of the information required the LAWtrust OA shall send a revocation request to the LAWtrust Root CA 2048 during a formal trusted ceremony at the LAWtrust vault in the hosted data centre.

The LAWtrust Root CA 2048 receiving the revocation request shall, immediately upon receiving such revocation, post the serial number of the revoked LAWtrust Subordinate CA Certificate to the CRL in the LAWtrust repository,

http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl.

If a LAWtrust Subordinate CA Certificate is revoked for any reason, the LAWtrust OA shall make a commercially reasonable effort to notify all PKI participants.

4.9.4 Revocation request grace period

In the case of a private key compromise or suspected private key compromise, LAWtrust shall request revocation of the associated LAWtrust Subordinate CA Certificate immediately upon detection of the compromise or suspected compromise.

Revocation requests for other required reasons shall be made as soon as reasonably practicable.

4.9.5 Time within which CA must process the revocation request

The LAWtrust Root CA 2048 shall use commercially reasonable efforts to issue CRL's at least once every 180 days. In certain circumstances CRL's may also be issued between these intervals, such as in the event of detection of a serious compromise. The issuance of LAWtrust Root CA 2048 CRL's will be performed during trusted ceremonies at the LAWtrust vault in the hosted data centre.

4.9.6 Revocation checking requirement for Relying Parties

Relying parties shall check CRL's on a daily basis to ensure reliance on LAWtrust Subordinate CA Certificates.

4.9.7 Bulk revocation requests

The LAWtrust Root CA 2048 shall not revoke LAWtrust Subordinate CA Certificates in bulk. LAWtrust Subordinate CA Certificates will be revoked individually following the process described in 4.9.3.

4.9.8 On-line revocation/status checking availability

A Relying Party shall check whether the LAWtrust Subordinate CA Certificate that the Relying Party wishes to rely on has been revoked. A Relying Party shall check the CRL's maintained in the appropriate repository to determine whether the LAWtrust Subordinate CA Certificate that the Relying Party wishes to rely on has been revoked. In no event shall LAWtrust or any sub-contractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable for any damages whatsoever due to:

- The failure of a Relying Party to check the revocation or expiry of a LAWtrust Subordinate CA Certificate; or
- Any reliance by a Relying Party on a LAWtrust Subordinate CA Certificate that has been revoked or that has expired.

4.9.9 On-line revocation checking requirements

No stipulation.

4.9.10 Other forms of revocation advertisements available

The CRL in the LAWtrust repository contains the revoked LAWtrust Subordinate CA Certificates and these may be searched by their serial numbers. No other mechanisms are provided.

4.9.11 Special requirements key compromise

If LAWtrust suspects or knows that a private key corresponding with the public key contained in LAWtrust Subordinate CA Certificate has been compromised, the LAWtrust OA shall inform the Security Committee using the procedures set out in 4.9.3, of such suspected or actual compromise.

LAWtrust shall immediately stop using the LAWtrust Subordinate CA Certificate and shall remove such LAWtrust Subordinate CA Certificate from any devices and/or software on which the LAWtrust Subordinate CA Certificate has been installed;

LAWtrust shall be responsible for investigating the circumstances of such compromise or suspected compromise and for notifying the LAWtrust Root CA 2048 and any Relying Parties that may have been affected by such compromise or suspected compromise.

4.9.12 Circumstances for suspension

The LAWtrust Root CA 2048 will under no circumstances suspend a LAWtrust Subordinate CA Certificate. The LAWtrust Root CA 2048 will under no circumstances perform bulk suspension of LAWtrust Subordinate CA Certificates.

4.10 Certificate status services

The LAWtrust Root CA 2048 shall maintain a CRL with a validity of 180 (one hundred and eighty) days.

The LAWtrust Root CA 2048 shall reissue CRL's from time to time to ensure the availability of service for parties relying on the CRL.

4.11 Issuing CA key archival and destruction

The LAWtrust Subordinate CA's, signed in the trust hierarchy of the LAWtrust Root CA 2048, are required to archive key pairs as part of their backup and archiving procedures. The LAWtrust Root CA 2048 will notify a PKI Participants when the LAWtrust Subordinate CA certificate has been revoked or has expired. On receipt of such a notification from the LAWtrust Root CA 2048, the LAWtrust Subordinate CA will implement procedures specified in the specific LAWtrust Subordinate CA CPS to securely destroy all archived copies of the LAWtrust Subordinate CA key pairs.

4.12 Key escrow and recovery policy and practices

The LAWtrust Root CA 2048 may provide a key escrow service under the control of the LAWtrust OA for Issuing CA's

The LAWtrust OA may provide key escrow services in accordance with the processes approved by the LAWtrust PA.

Keys shall only be recovered for purposes of disaster recovery and immediately they are no longer required for this purpose shall be destroyed save in the instance of LAWtrust Subordinate CA Certificates which provide encryption only.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Entrust Authority Security Manager is used as the software component of the LAWtrust Root CA 2048.

5.1.1 Site location and construction

The offline LAWtrust Root CA 2048 hardware and software are hosted in a LAWtrust Vault at the hosted data centre with physical security and access control procedures that meet or exceed industry standards.

5.1.2 Physical access

Physical access to the LAWtrust Root CA 2048 is strictly controlled. Only authorised LAWtrust representatives can gain access to the LAWtrust biometric vault at the hosted data centre and they are identified by biometric access control to the data centre, physical keys and biometric access the LAWtrust bio-vault and physical keys to the LAWtrust Certificate Authority rack within the bio-vault. To access the LAWtrust Root CA 2048 server in the LAWtrust hosted data centre a minimum of two authorised LAWtrust representatives are required, one to open the bio-vault with biometric and physical key and one to open the Certificate Authority rack within the bio-vault.

5.1.3 Network and CA server security

The LAWtrust Root CA 2048 hosted in the LAWtrust bio-vault at the hosted data centre is an offline CA and when operational is not connected to a network. The virus and other malicious software detection and prevention tools as described in the LAWtrust Information Security Policy will be installed on the LAWtrust Root CA 2048 server or the media used to transfer any material to and from the Root CA is only used on servers with antivirus and the media is stored in the Safe when not used.

5.1.4 Air conditioning

The hosted data centre where the LAWtrust Root CA 2048 is hosted is fully air-conditioned.

5.1.5 Water exposures

The hosted data centre is protected against water exposure.

5.1.6 Fire prevention and protection

The data centre facility is fully wired for fire detection and alarm. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.7 Media storage

All backup media is stored in a separate location that is physically secure and protected from fire and water damage.

5.1.8 Waste disposal

Waste is removed or destroyed in accordance with industry best practice. Media used to store sensitive data is destroyed, such that the information is unrecoverable, prior to disposal.

5.1.9 Off-site backup

Backups are stored in the LAWtrust PKI Safe in the LAWtrust House data centre.

5.2 Procedural controls

The LAWtrust Root CA 2048 has a number of trusted roles for sensitive operations of the software used to facilitate the issuance of LAWtrust Subordinate CA certificates.

To gain access to the software used by the LAWtrust Root CA 2048 operational personnel must undergo background investigations.

5.2.1 Trusted Roles

LAWtrust has identified a number of roles which contribute to the integrity of the LAWtrust Root CA 2048 and require a high level of trust. A list of these roles is provided below.

5.2.1.1 LAWtrust Root CA 2048 Roles

- First Officer: Security Officer as defined in the CA documentation
- Master User 1, 2 and 3: start and stop CA services and other sensitive CA activities

- System Administrators: Administration of the operating system
- Cryptographic custodian: Person safekeeping cryptographic material.
- Witnesses: Persons performing witness roles of sensitive activities.

5.2.1.2 nShield Hardware Security Module Roles

- Administrator Card Holders – Sensitive key management and recovery operations
- Operator Card Holders – Activation of the CA private signing key.

5.2.2 Number of persons required per task

The LAWtrust Root CA 2048 private signing key is only unencrypted in the FIPS 140-2 level 3 boundary of the nShield Edge HSM. To access the CA key material a minimum of three Operator Card Holders are required. The activation of the LAWtrust Root CA 2048 private key through the nShield Edge HSM requires three persons All CA roles are assigned strictly according to the prescriptions of the CA specifications.

5.2.2.1 nShield Edge Hardware Security Module Roles

- Administrator Card holders: 2 of 3.
- Operator Card holders: 3 of 3.

5.2.2.2 Entrust Authority Security Manager Roles

All roles: either 1 of 1 (first officer) or 1 of 3 (master users) or 1 of 1 (CA user - Server Administrator).

5.2.3 Roles requiring segregation of duties

LAWtrust enforces a strict segregation of duties with regards to key management activities. The segregation of duties and the trusted role delegation is handled by the LAWtrust Operating Authority and the LAWtrust Key Manager. The LAWtrust Root CA 2048 key material can only be accessed by authorised LAWtrust operational personnel and is physically separated from the LAWtrust CA operational environment.

5.3 Personnel controls

Operational personnel of the LAWtrust Root CA 2048 will not be assigned responsibilities that conflicts the segregation of duties requirements of the LAWtrust Root CA 2048. The operational personnel for the LAWtrust Root CA 2048 shall be assigned privileges limited to the minimum required to carry out their assigned duties.

The operational personnel for the LAWtrust Root CA 2048 will be adequately trained to perform CA duties in a professional and skilled manner. An in-house development PKI training course and CA product training will be used for this purpose.

Only LAWtrust employees, duly authorised by the LAWtrust OA, will perform the following CA functions:

- Control or set Root CA Policy
- Set or restore the CA Security Policy
- Sign LAWtrust Subordinate CA Certificates
- Import certificate definitions/specifications

5.4 Audit logging procedures

Significant security events in the LAWtrust Root CA 2048 are automatically time-stamped and recorded as audit logs in audit trail files when the CA is operational. The audit trail files are processed (reviewed for policy violations or other significant events) when the Root CA 2048 is powered on for CRL signing, LAWtrust Subordinate CA signing or revocation. Only authorised CA personnel operating under the LAWtrust Root CA 2048 can view the audit trail files. The integrity of the audit files are protected against modification using digital signatures with the LAWtrust Root CA 2048 private signing key. Audit trail files are backed up and archived periodically. All files including the latest audit trail file are moved to backup media (USB) and stored in the LAWtrust PKI Safe in the data centre.

5.5 Records archival

The audit trail files and databases for LAWtrust Root CA 2048 are both archived. The archives of the LAWtrust Root CA 2048's database are retained for at least 7 (seven) years. Archives of audit trail files are retained online for at least 1 (one) year and will be included in the CA Archive information. The database for LAWtrust Root CA 2048 is encrypted and protected by the CA software master keys. Archive files are stored at a secure and separate geographic location as described in 5.4.

5.6 Key changeover

LAWtrust Subordinate CA Certificates expire after a defined period of time to minimize the exposure of the associated key pair. For this reason, a new key pair must be created and that new public key must be submitted with each LAWtrust Subordinate CA Certificate request to replace an expiring LAWtrust Subordinate CA Certificate.

LAWtrust Root CA 2048's key pair will be retired from service at the end of their lifetime as defined in 6.5.3. A new Root CA key pair will be created as required to support the continuation of LAWtrust Subordinate CA Services. The LAWtrust Root CA 2048 will continue to publish CRLs signed with the original key pair until all LAWtrust Subordinate CA certificates issued using that original key pair has expired. The LAWtrust Root CA 2048 key changeover process will be performed such that it causes minimal disruption to PKI participants and Relying Parties.

5.7 Compromise and disaster recovery

The LAWtrust Root CA 2048 has a disaster recovery plan as part of its business continuity strategy to provide for timely recovery of services in the event of a system outage. The LAWtrust Disaster Recovery Plan is an internal document and will be discussed with PKI Participants on request. The disaster recovery procedures include the timeframes for recovery as well as information on the location of the disaster recovery site.

Rigorous security controls are required to maintain the integrity of the LAWtrust Root CA 2048. The compromise of the private key used by the LAWtrust Root CA 2048 is viewed

as being very unlikely; however, LAWtrust has policies and procedures that will be employed in the event of such a Compromise. At a minimum, all PKI Participants shall be informed as soon as practicable of such a Compromise and information shall be posted in the LAWtrust Repository.

5.8 LAWtrust Root CA 2048 termination

In the event that the LAWtrust Root CA 2048 ceases operation, all the LAWtrust Subordinate CA Certificates will be revoked by the LAWtrust Root CA 2048. If LAWtrust believes that there is a risk that the LAWtrust Root CA 2048 private key has been compromised, then LAWtrust will immediately declare a disaster and follow the CA key compromise procedures set out in the disaster recovery plan.

5.9 LAWtrust Root CA 2048 impact on third party functionality

Certificates issued by the LAWtrust Root CA 2048 will not alter or negatively impact the functionality of any operating system or any third-party software in any manner.

5.10 Escalation of physical security violations

All physical security incidents and violations have to be reported to the LAWtrust OA and PA as a matter of urgency.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

The signing key pair for the LAWtrust Root CA 2048 was created during the initial start up of the CA request and is protected by the master keys for the LAWtrust Root CA 2048. Hardware key generation is used which is compliant to FIPS 140-2 level and uses FIPS 186-2 key generation techniques.

6.2 CA key pair usage

The LAWtrust Root CA 2048 private signing keys are used for signing LAWtrust Subordinate CA Certificates and Certificate Revocation Lists exclusively.

6.3 Private key delivery

LAWtrust shall be responsible for the generation and safeguarding of its private keys unless otherwise required and approved by the LAWtrust PA.

6.4 Public key delivery to certificate issuer

The public key to be included in a LAWtrust Subordinate CA Certificate is delivered to the LAWtrust Root CA 2048 in a Certificate Signing Request (CSR) as part of the LAWtrust Subordinate CA Certificate request process included in a formal key generation ceremony.

6.5 CA public key delivery to Relying Parties

The LAWtrust Root CA 2048's public key can be obtained from the any of the chained LAWtrust Subordinate CA's or from the LAWtrust Repository at [https://www.lawtrust.co.za/repository].

6.5.1 Key sizes

The LAWtrust Root CA 2048 will have a key size of 2048-bit RSA. All new LAWtrust Subordinate CA's shall have a minimum key size of 2048-bit RSA.

The LAWtrust PA will perform an annual review on the LAWtrust Root CA 2048' private key lengths to determine the appropriate key usage period considering any new developments on the analysis of RSA private keys. The review process is stipulated in the LAWtrust PA procedures.

6.5.2 Key usage purposes (as per X.509 v3 key usage field)

LAWtrust Subordinate CA Certificates issued by the LAWtrust Root CA 2048 contain the key usage and enhanced usage certificates and extensions restricting the purpose for which the LAWtrust Subordinate CA Certificate can be used. LAWtrust and Relying Parties

shall only use LAWtrust Subordinate CA Certificates in compliance with the LAWtrust Root CA 2048 CPS and applicable laws.

6.5.3 Other key management aspects

The LAWtrust Root CA 2048 RSA key pair expires on 16 May 2032.

6.6 Private key protection and cryptographic module engineering controls

The LAWtrust Root CA 2048 uses the CA software in conjunction with hardware certified to FIPS 140-2 Level 3 to protect the private keys. The LAWtrust Root CA 2048's private keys are backed up and require a minimum of two HSM key share-holders to be accessed or recovered. The LAWtrust Root CA 2048's private keys will be destroyed according to the processes set out in the LAWtrust Hardware Disposal Policy. LAWtrust do not outsource key escrow of the LAWtrust Root CA 2048's private keys and no third parties have access to the LAWtrust Root CA 2048's private keys.

6.7 CA certificate re-key

The self-signed LAWtrust Root CA 2048 contains an expiration date. When the LAWtrust Root CA 2048 reaches this expiration date, LAWtrust will re-key the LAWtrust Root CA 2048. LAWtrust shall make a commercially reasonable effort to notify all PKI Participants of the pending expiration of the LAWtrust Root CA 2048 certificate. A notification will also be published in the LAWtrust Repository. Upon expiration of the LAWtrust Root CA 2048 certificate, all PKI Participants shall immediately cease using the certificate and shall remove the LAWtrust Root CA 2048 certificate from any devices and/or software in which it has been installed.

6.8 Computer security controls

The server on which the LAWtrust Root CA 2048 operates is offline and physically secured as described in 5.1 of the LAWtrust Root CA 2048 CPS. The operating systems on the server on which LAWtrust Root CA 2048 operate enforces identification and authentication of users. Access to the CA software databases and audit trails is restricted

as described in the LAWtrust Root CA 2048 CPS. All operation personnel that are authorised to have physical access to the LAWtrust Root CA 2048 are required to use physical keys in conjunction with a biometric authentication to gain access to the LAWtrust hosted vault and physical key to access the Certificate Authority rack where the LAWtrust Root CA 2048 is stored. Physical access to the LAWtrust hosted vault where the CA equipment and the CA software are located is described in 5.1.2.

6.9 Life cycle technical controls

The efficacy and appropriateness of the security settings described in the LAWtrust Root CA 2048 CPS are reviewed on a yearly basis. A risk and threat assessment will be performed to determine if key lengths need to be increased or operational procedures modified from time to time to maintain system security.

6.10 Information security

The LAWtrust Root CA 2048 shall be subject to generally accepted information security practice as documented in the LAWtrust Information Security Policy.

6.11 Escalation of information security violations

All information security incidents and violations, including technical and physical access incidents, have to be reported to the LAWtrust OA and PA as a matter of urgency.

7. CERTIFICATE PROFILES

7.1 Certificate profile

The profile of a LAWtrust Subordinate CA certificate, approved by the LAWtrust PA, will be governed by the profile given below.

- Version: set to v3
- Serial number: unique 32-bit non-negative integer
- Signature algorithm: SHA1RSA,SHA256 after 2016-12-31.
- Issuer: CN=LAWtrust Root Certification Authority 2048,OU=LAW Trusted Third Party Services PTY Ltd.,O=LAWtrust,C=ZA
- Validity period: 10 years, or the maximum of (5 and the Root valid until date–current year).
- Subject: Unique X.500 CA Distinguished Name (CN=[LAWtrust Certification Authority 2048], OU = LAW Trusted Third Party Services PTY Ltd.,O = LAWtrust,C = ZA
- Public key information: 2048-bit RSA
- Key usage: Certificate Signing, Off-line CRL Signing, CRL Signing
- CRL distribution points: URL= http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl and LDAP URL = ldap:// CN=CRL1,CN=LAWtrust Root Certification Authority 2048,OU=LAW Trusted Third Party Services PTY Ltd.,O=LAWtrust,C=ZA
- Authority key identifier: 20 byte SHA-1 hash of the Issuer's public key

- Subject key identifier: 20 byte SHA-1 hash of the Subject's public key
- Certificate policies: URL: [https://www.lawtrust.co.za/repository] and short reference to terms & conditions
- Basic constraints: Subject Type = CA & Path Length Constraint = None

7.2 CRL profile

The profile of a LAWtrust CRL, approved by the LAWtrust PA, will be governed by the profile given below:

- Version: set to v2
- Signature algorithm: SHA1RSA
- Issuer: CN=LAWtrust Certification Authority 2048,OU=LAW Trusted Third Party Services PTY Ltd.,O=LAWtrust,C=ZA
- Effective date: Time of current CRL issuance
- Next update: Time of next expected CRL issuance
- CRL number: unique 32-bit non-negative integer
- Authority key identifier: 20 byte SHA-1 hash of the Issuer's public key
- Revoked certificates: List of serial numbers of revoked certificates

7.3 OCSP profile

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The LAWtrust Root CA 2048 shall be audited for compliance against the practices and procedures set forth in the LAWtrust Root CA 2048 CPS, the WebTrust standard and the SANS21188 standard. This will include:

- LAWtrust Root CA 2048 Business Practices Disclosure;
- Service Integrity;
- LAWtrust Root CA 2048 Environmental Controls.

8.1 Frequency or circumstances of assessment

The LAWtrust Root CA 2048 shall be audited once per calendar year for compliance with the practices and procedures set out above. If the results of an audit report recommend remedial action, LAWtrust shall initiate corrective action within 30 (thirty) days of receipt of such audit report.

8.2 Identity/qualifications of assessor

A compliance audit shall be performed by a firm with demonstrated competency in the evaluation of certification authorities and registration authorities against the above specified audit criteria.

8.3 Assessor's relationship to assessed Entity

The Entity selected to perform the compliance audit for the LAWtrust Root CA 2048 shall be independent from the Entity being audited.

8.4 Topics covered by assessment

The compliance audit shall test compliance of the LAWtrust Root CA 2048 against the requirements set out above.

8.5 Actions taken as a result of deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited LAWtrust Root CA 2048 shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

8.6 Communication of results

The result of all compliance audits shall be communicated to the LAWtrust OA, LAWtrust PA and the LAWtrust Board of Directors on completion of the audit.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No stipulation

9.2 Confidentiality of business information

LAWtrust shall use commercially reasonable care to prevent such information from being used or disclosed for purposes other than those described in the LAWtrust Root CA 2048 CPS or Relying Party Agreement. Notwithstanding the foregoing Applicants and Subscribers acknowledge that some of the information supplied with a LAWtrust Subordinate CA Certificate request is incorporated into a LAWtrust Subordinate CA Certificate and that the LAWtrust Root CA 2048, the LAWtrust OA and any other parties authorised by LAWtrust to do so shall be entitled to make such information publicly available.

9.2.1 Scope of confidential information

Information that is supplied by Applicants, Subscribers or Relying Parties for the subscription for, use of, or reliance upon a LAWtrust Subordinate CA Certificate, and which is not included in the information described in 9.2.2 below, shall be considered to be confidential. The LAWtrust Root CA 2048 and the LAWtrust OA shall be entitled to

disclose such information to any sub-contractors or agents that are assisting LAWtrust in the authentication of the identity of the Applicant and the verification of information supplied in LAWtrust Subordinate CA Certificate requests or that are assisting LAWtrust in the operation of the LAWtrust Root CA 2048 or the LAWtrust OA. Information considered to be confidential shall not be disclosed unless compelled, pursuant to legal, judicial or administrative proceedings, or otherwise required by law. The LAWtrust Root CA 2048 and the LAWtrust OA shall be entitled to disclose information that is considered to be confidential to legal and financial advisors assisting in connection with any such legal, judicial, administrative or other proceedings required by law, and to potential acquirers, legal counsel, accountants, bank and financing sources and other advisors in connection with mergers, acquisitions and re-organisations.

9.2.2 Information not within the scope of confidential information

Information that is included in a LAWtrust Subordinate CA Certificate or a LAWtrust Revocation List shall not be considered confidential.

Information contained in the LAWtrust Root CA 2048 CPS shall not be considered confidential.

Without limiting the foregoing, the following information shall not be considered confidential. Information that:

- Was or becomes known through no fault of LAWtrust;
- Was rightfully known or becomes rightfully known to LAWtrust without confidential or proprietary restriction from a source other than LAWtrust;
- Is independently developed by LAWtrust; or
- This information does not include information that is classified as Personal Information by the Protection of Personal Information Act (POPI), other than the information already indicated in this document to be disclosed.

9.2.3 Responsibility to protect confidential information

LAWtrust shall use commercially reasonable care to prevent its confidential information from being used or disclosed for purposes other than set out in the LAWtrust Root CA 2048 CPS or Relying Party Agreements.

9.3 Privacy of personal information

Privacy of personal information shall be protected in terms of POPI and the process of dealing with personal information, is published in the LAWtrust Privacy Notice published on the LAWtrust Website at [https://www.lawtrust.co.za/repository].

9.4 Intellectual property rights

LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under the LAWtrust Subordinate CA Certificate(s).

LAWtrust grants permission to reproduce the LAWtrust Root CA 2048 CPS provided that:

- The copyright notice on the first page of the LAWtrust Root CA 2048 CPS is retained on any copies of the CPS; and
- The LAWtrust Root CA 2048 CPS is reproduced fully and accurately. LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under the LAWtrust Root CA 2048 CPS.

In no event shall LAWtrust or any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable to any Applicants, Subscribers, or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or any other right of person, Entity, or organization in any jurisdiction arising from or relating to any LAWtrust Subordinate CA Certificate or arising from or relating to any services provided in relation to any LAWtrust Subordinate CA Certificate.

9.5 LAWtrust Root CA 2048 representations and warranties

LAWtrust makes the following limited warranties with respect to the operation of LAWtrust Root CA 2048:

- LAWtrust Root CA 2048 shall provide Repository services consistent with the practices and procedures set forth in the LAWtrust Root CA 2048 CPS;
- LAWtrust Root CA 2048 shall perform LAWtrust Subordinate CA Certificate issuance consistent with the procedures set forth in the LAWtrust Root CA 2048 CPS; and
- LAWtrust Root CA 2048 shall provide revocation services consistent with the procedures set forth in the LAWtrust Root CA 2048 CPS.

Notwithstanding the foregoing, in no event does LAWtrust, or the LAWtrust OA or the employees, or directors of LAWtrust make any representations, or provide any warranties, or conditions to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to:

- The techniques used in the generation and storage of the private key corresponding to the public key in a LAWtrust Subordinate CA Certificate, including, whether such private key has been Compromised or was generated using sound cryptographic techniques,
- The reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing a LAWtrust Subordinate CA Certificate,
- Any software whatsoever, or
- Non-repudiation of any LAWtrust Subordinate CA Certificate or any transaction facilitated through the use of a LAWtrust Subordinate CA Certificate, since such determination is a matter of applicable law.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to LAWtrust Subordinate CA Certificates and request using LAWtrust Subordinate CA Certificates are dependent on the transmission of information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of LAWtrust or a LAWtrust RA or the employees, or directors of LAWtrust or a LAWtrust RA. Neither LAWtrust nor any LAWtrust RA or employees, or directors of LAWtrust, shall be liable for any error, failure, delay, interruption, defect, or corruption in relation to a LAWtrust Subordinate CA Certificate, a LAWtrust Subordinate CA Certificate CRL, or a LAWtrust Subordinate CA Certificate request to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

9.6 LAWtrust RA representations and warranties

The same liability provisions that apply in Section 9.5 with respect to LAWtrust Root CA 2048 shall apply with respect to LAWtrust OA and employees, and directors of the foregoing.

9.7 LAWtrust representations and warranties

LAWtrust represent and warrant that:

- Where applicable, the private key corresponding to the public key submitted by LAWtrust in connection with a LAWtrust Subordinate CA Certificate request was created using sound cryptographic techniques and has not been compromised;
- Any information provided by LAWtrust does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, Entity, or organization in any jurisdiction;
- LAWtrust shall immediately cease to use the LAWtrust Subordinate CA Certificate if any information included in the LAWtrust Subordinate CA Certificate changes or

if any change in any circumstances would make the information in the LAWtrust Subordinate CA Certificate misleading or inaccurate;

- LAWtrust shall immediately cease to use the LAWtrust Subordinate CA Certificate upon:
  - Expiration, suspension or revocation of the LAWtrust Subordinate CA Certificate, or
  - Any suspected or actual compromise of the private key corresponding to the public key in such LAWtrust Subordinate CA Certificate, and shall remove such LAWtrust Subordinate CA Certificate from the devices and/or software in which it has been installed.
- LAWtrust Shall not use the LAWtrust Subordinate CA Certificates for any hazardous or unlawful activities.

9.8 Relying party representations and warranties

Relying Parties represent and warrant to LAWtrust that:

- The Relying Party shall properly validate a LAWtrust Subordinate CA Certificate before making a determination about whether to rely on such LAWtrust Subordinate CA Certificate, including confirmation that the LAWtrust Subordinate CA Certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root;
- The Relying Party shall not rely on a revoked or expired LAWtrust Subordinate CA Certificate;
- The Relying Party shall not rely on a LAWtrust Subordinate CA Certificate that cannot be validated back to a trustworthy root;

- The Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on a LAWtrust Subordinate CA Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by a LAWtrust Subordinate CA Certificate and the importance or value of any transaction that may involve the use of a LAWtrust Subordinate CA Certificate; and

- The Relying Party shall not use a LAWtrust Subordinate CA Certificate for any hazardous or unlawful activities.

9.9 Disclaimers of warranties

Except as specifically provided in sections 9.5 and 9.6, neither LAWtrust, the LAWtrust Root CA 2048 nor the LAWtrust OA nor the employees, or directors of any of the foregoing shall make any representations or give any warranties or conditions, whether express, implied, statutory, by usage of trade, or otherwise, and LAWtrust and the employees, and directors of the foregoing specifically disclaim any and all representations, warranties, and conditions of merchantability, non-infringement, title, satisfactory quality, and/or fitness for a particular purpose.

While LAWtrust makes every effort to ensure that all information provided by LAWtrust is correct and does not contain any errors, omissions, or misrepresentations, LAWtrust cannot issue any warranties in this regard.

9.10 Limitation of liability

Neither LAWtrust, nor the LAWtrust OA, nor the employees, or directors of any of the foregoing entities shall be liable for any (a) direct, (b) indirect or special damages and/or (c) loss of income or profit and/or (d) any other form of consequential damages howsoever arising, and regardless of form or cause of action. There are no financial responsibilities from subcontractors, vendors, suppliers, representatives and agents with regards to the certificate services provided by LAWtrust.

9.11 Force Majeure

Neither LAWtrust, nor the employees, or directors of any of the foregoing entities shall be in default hereunder, or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from a failure to perform or comply with the terms of the LAWtrust Root CA 2048 CPS, or any Relying Party Agreement due to any causes beyond its control, which causes include, but are not limited to acts of God or of the public enemy, riots or insurrections, war, accidents, fire, strikes and other labour difficulties, embargoes, judicial action, default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labour, materials, energy, utilities, components for machinery, acts of civil or military authorities.

9.12 Individual notices and communications with participants

Unless expressly agreed with any participant to the contrary in writing, or stipulated by the LAWtrust PA to the contrary, communications addressed to a participant by LAWtrust, may, at the foregoing discretion, be communicated by eMail to the eMail address provided by the participant.

9.13 Amendments

9.13.1 Process for amendments

- LAWtrust PA shall consider the provisions of the LAWtrust Root CA 2048 CPS, any documents, including without limitation a Relying Party Agreement, previously approved by the LAWtrust PA at least annually and shall also consider proposals for amendment that may be received from the LAWtrust OA.

- A proposal for an amendment to the LAWtrust Root CA 2048 CPS or to any documents, including without limitation, a Relying Party Agreement, previously approved by the LAWtrust PA shall be submitted to the LAWtrust PA for consideration.

- The LAWtrust PA shall within a period of not more than 60 (sixty) days from the date of receipt of the proposal, consider the proposal and determine whether the proposal for amendment is well founded and an amendment warranted.

- Once an amendment has been drafted it shall be considered by the LAWtrust PA taking into account good practice relating to the PKI, information security and the needs and best interests of the participants to the PKI.

9.13.2 Notification mechanism and period

- The LAWtrust PA shall determine the notification mechanisms and period before which an amendment may become effective in each instance and provide written directives in this regard.

- The LAWtrust PA shall exercise reasonable care to ensure that the mechanism of notification and the period of notification do not prejudice participants in the PKI and are in the best interests of the proper and secure operation of the PKI.

9.14 Dispute resolution

In cases of policy disputes, the LAWtrust Policy Authority will be responsible for dispute resolution. The LAWtrust Managing Director will be responsible for financial disputes. If the matter in dispute is primarily a legal matter then the Arbitrator shall be a person of relevant experience, making use of the simplified Rules of the Arbitration Foundation of Southern Africa (AFSA) and shall be appointed by agreement between the parties. If the parties are unable to agree as to the appointment of an Arbitrator within 7 (seven) days of the arbitration being demanded by any party, then he shall be appointed by the Secretariat of AFSA within 7 (seven) days of being requested to do so by any party. Should the Arbitrator deem it necessary to obtain technical advice on any matter relating to the dispute he shall be entitled to obtain such advice from a technical expert in the relevant field.

In cases of technical disputes, the LAWtrust Operations Authority will be responsible for dispute resolution in consultation with the LAWtrust Policy Authority. If the matter in

dispute is primarily a technical matter, then the Arbitrator shall be an expert in the matter under dispute appointed by agreement between the parties. If the parties are unable to agree as to the appointment of an Arbitrator within 7 (seven) days of the arbitration being demanded by any party, then he shall be appointed by the Chairman at the time of the Computer Society of South Africa within 7 (seven) days of being requested to do so by any party.

9.15 Governing law

The entire provisions of the LAWtrust Root CA 2048 CPS and Relying Party Agreement entered into pursuant to the LAWtrust Root CA 2048 CPS shall be governed by and construed in accordance with the laws of the Republic of South Africa. Furthermore, the parties hereto irrevocably and unconditionally consent to the non-exclusive jurisdiction of the Johannesburg Magistrate's Court or the South Gauteng Division of the High Court of South Africa, as the case may be, in regard to the enforcement of any rights relating to all matters arising from the LAWtrust Root CA 2048 CPS.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The provisions of the LAWtrust Root CA 2048 CPS or Relying Party Agreements, as the case may be, constitute the entire contract between the applicable parties with regard to matters dealt with in the LAWtrust Root CA 2048 CPS and those agreements. No representations (save for any fraudulent misrepresentations) terms, conditions or warranties not contained in the LAWtrust Root CA 2048 CPS or Relying Party Agreements, as the case may be, shall be binding on the parties.

9.16.2 Severability

To the extent that any provisions of the LAWtrust Root CA 2048 CPS or Relying Party Agreements, as the case may be, may be struck-out as unlawful, only those provisions shall be severed from the LAWtrust Root CA 2048 CPS or Relying Party Agreements and

all other provisions of the LAWtrust Root CA 2048 CPS or Relying Party Agreements shall remain of full force and effect, notwithstanding the severing of those provisions.

9.16.3 Merger

The LAWtrust Root CA 2048 CPS (LAWtrust Root CA 2048) and the Relying Party Agreements state all of the rights and obligations of LAWtrust, any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing, and any Applicant, Subscriber, or Relying Party and any other persons, entities, or organizations in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications, or understandings of any nature whatsoever whether oral or written.

The rights and obligations of LAWtrust, any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, and directors of any of the foregoing may not be modified or waived orally and may be modified only in a writing signed or authenticated by a duly authorized representative of LAWtrust.

In the event of a merger with any other company of acquisition of LAWtrust, the provisions of the LAWtrust Root CA 2048 CPS, will continue on as stated herein, unless and until a change or deviation therefrom is communicated though one of the mechanisms contained herein.

10. SIGN OFF ACCEPTANCE

Name:	Katekani Hlabathi
Authority:	Policy Authority
Title:	Chief Information Officer
Date:	2018-12-14
Signature: