LAWTRUST ROOT CA 2048

CERTIFICATION PRACTICE STATEMENT

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	Expired
V010 2020-08-07	2020-08-07	Katekani Hlabathi	2020 Review	Expired
V011 2021-08-05	2021-08-05	Katekani Hlabathi Mmabatho Masemene Marcile De Waal	Updated the CPS to conform to RFC3647 Standard	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	**Error! Unknown document property name.**	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

Document Control

This document shall be reviewed annually and an update by LAWtrust may occur earlier if internal or external influences affect its validity.

Digitally Signed Copy of this document shall be stored at LAWtrust Document Store.

Table of Contents

1 INTRODUCTION

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by LAWtrust Root CA 2048. In particular, this CPS establishes the processes and procedures the LAWtrust Root CA 2048 follow to:

- Issue LAWtrust compliant certificates to LAWtrust subordinate Issuing Certificate Authorities (Sub-CAs) that it signs;
- Manage certificate life cycle for the Sub-CA and end entity certificates issued under the LAWtrust PKI CA hierarchy;
- Operate a directory of issued sub-CA certificates; and
- Operate the CRL directory.

LAWtrust Root CA 2048 is hosted in the LAWtrust data centre which is responsible for managing LAWtrust Root CA 2048 operations.

This CPS complies with the stipulations of the LAWtrust Certificate Policy (CP) and in line with Internet Request for Comment (RFC) 3647 [RFC 3647]. Sections that are not applicable to LAWtrust Root CA 2048 are labelled “No Stipulation”

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 subordinate 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.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by LAWtrust Root CA 2048 to sub-CAs will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a certificate is trusted for a particular purpose.

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the LAWtrust Root CA 2048 as governed by LAWtrust CP and related documents which describe LAWtrust Root CA 2048 requirements and use of Certificates.

1.1.3 SCOPE

This CPS applies to Subordinate CA certificates issued by the LAWtrust Root CA 2048.

LAWtrust operates a Public Key Infrastructure (FPKI) under the two Root CAs (LAWtrust Root CA 2048 and LAWtrust Root CA02 (4096). The LAWtrust PKI has core offerings of public key infrastructure (PKI) services and digital trust services designed to enable electronic signature for business entities and individuals.

Under the LAWtrust Root CA 2048, there are Subordinate Issuing Certificate Authorities (Sub-CAs) that issue certificates to end subscribers, herein referred to as Issuing CAs. The three Issuing CAs are the LAWtrust AeSign Certification Authority 2048, LAWtrust AeSign CA02 and the LAWtrust AATL CA. The full hierarchy of the LAWtrust PKI is indicated in Figure 1.

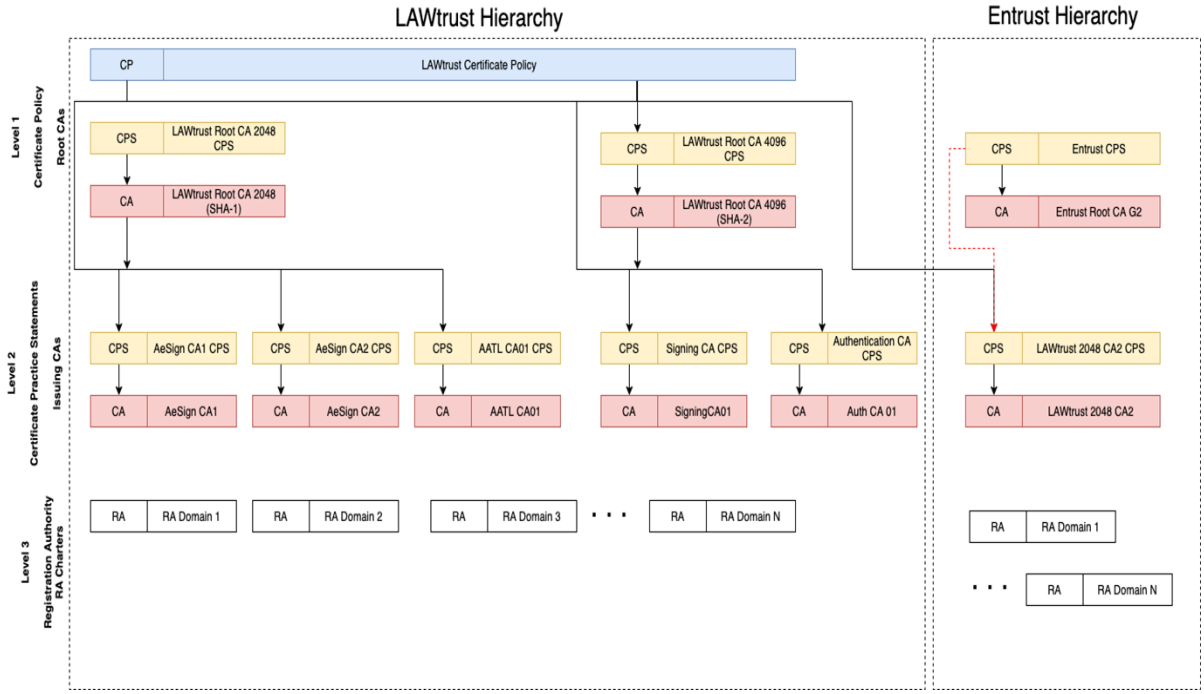

Figure 1. LAWtrust PKI

1.2 DOCUMENT NAME AND IDENTIFICATION

This document title is "LAWtrust Root Certification Practice Statement (LAWtrust Root CA 2048 CPS)" and is identified by the following object identifier (OID):

OID: 1.3.6.1.4.1.54383.1.1

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 Certification Authority 2048
- LAWtrust AeSign CA02
- LAWtrust AATL CA01

1.3.3 LAWTRUST POLICY AUTHORITY (LAWTRUST PA)

The LAWtrust Policy Authority (LAWtrust PA) is an assigned role responsible for the governance of the LAWtrust PKI. The LAWtrust PA is responsible for the following:

- Ensuring the operation of the LAWtrust PKI CA comply with the requirements of the LAWtrust CP, applicable CPS and LAWtrust Information Security Policy;
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the LAWtrust PKI specific business requirements;
- Seeking resolution of disputes between participants operating in its domain;

1.3.4 REGISTRATION AUTHORITY (RA)

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

1.3.4.1 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.

1.3.4.2 Appointed Registration Authorities

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

1.3.5 LAWTRUST SECURITY COMMITTEE

LAWtrust Security Committee is responsible for the approval of PKI Policies and overseeing the security operations of the LAWtrust Root CA 2048.

1.3.6 SUBSCRIBERS

Subscribers are individuals (end users) or entities (organizations) to whom certificates are issued. Subscribers are bound by the conditions of use of certificates as contained in the Subscriber Agreement. In general, the subscriber asserts that he or she uses the key and certificate in accordance with the LAWtrust CP and this CPS.

1.3.7 RELYING PARTIES

A Relying Party in this context is the entity that relies on the validity of the binding of the LAWtrust Root CA 2048 identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the LAWtrust Root CA 2048. A Relying Party's right to rely on a certificate issued under this CPS, requirements for reliance, and limitations thereon, are governed by the terms of the LAWtrust CP and the Relying Party Agreement.

Relying Parties shall use the LAWtrust Root CA 2048, and rely on a certificate that has been issued under the LAWtrust CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the LAWtrust CP;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.8 ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER

Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. LAWtrust Root CA 2048 may make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The LAWtrust Root CA 2048 shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4 CERTIFICATE USAGE

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

1.4.1 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 CAs;
- Validating Certificate Revocation Lists issued by the LAWtrust Subordinate CAs.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CPS shall not be authorized for use in any circumstances or in any application which is illegal under South African law, could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines, and the LAWtrust Root CA 2048 shall not be liable for any claims arising from such use.

1.5 Policy Administration

1.5.1 Administration Organization

This CPS is administered by the LAWtrust PA (Policy Authority) and is based on policies established under the LAWtrust CP (see section 1.3.1).

1.5.2 Contact Person

Queries regarding LAWtrust Root CA 2048 CPS shall be directed at:

Email: governance@lawtrust.co.za

Telephone: +27126769240

Any formal notices required by this CPS shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CPS.

1.5.3 Person Determining CPS Suitability for the Policy

The LAWtrust PA is responsible for approving this CPS and establishing that the LAWtrust Root CA 2048 conform to the requirements of the LAWtrust CP in accordance with policies and procedures specified by LAWtrust.

1.5.4 CPS Approval

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, 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.

1.6 Definitions and Acronyms

The terms used in this document shall have the meanings as defined in the **Appendix A** of this document.

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;

a. 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.

b. Certificate Status Repository

The LAWtrust Subordinate CAs' 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.

2.1.1 Repository Obligations

The repository capabilities that LAWtrust Root CA 2048 will deploy shall include:

- LDAP Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3) or Hypertext Transfer Protocol (HTTP);
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CPS and LAWtrust CP; and
- Access control mechanisms when needed to protect repository availability and information.

The LAWtrust Root CA 2048 shall post CRLs to an LDAP directory and/or an HTTP-based web server. LAWtrust has instituted access controls, including strong authentication of authorized Relying Parties, to promote consistent access to LAWtrust Root CA 2048 issued certificates and CRLs and to prevent modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The LAWtrust Root CA 2048 maintain repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. LAWtrust Root CA 2048 shall be providing Relying Parties with information on how to find the appropriate repository to check certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the appropriate OCSP responder

LAWtrust Root CA 2048 repositories shall contain the following PKI related elements:

- Subordinate CA certificates: CA certificates shall be made internally available; and
- CRLs: CRLs shall be made publicly available to allow relying parties to verify the status of certificates.

The LAWtrust PA will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information.

2.2.2 Publication of CA Information

The LAWtrust Root CA 2048 CPS shall be made available to all LAWtrust PKI Participants at LAWtrust website https://www.lawtrust.co.za/repository at all times subject to any interruption of the LAWtrust website services or from LAWtrust in hardcopy upon request. This web site is the only source for up-to-date documentation and LAWtrust Root CA 2048 reserves the right to publish newer versions of the documentation without prior notice.

Additionally, the LAWtrust Root CA 2048 will publish an approved, current and digitally signed version of its CP and PDS.

LAWtrust private LDAP directory and the website https://www.lawtrust.co.za/repository are the only authoritative sources for:

- Al accessible certificates issued by LAWtrust Root CA 2048; and
- The certificate revocation list (CRL) for the LAWtrust Root CA 2048.

2.2.3 INTEROPERABILITY

Repository information is stored using technology that supports the following industry standards and schema:

- LDAP v3 operations;
- LDAP search filters;
- LDAP v3 intelligent referral;
- DSML (Directory Service Markup Language) v2;
- X.509 digital certificates;
- HTTP.

2.3 TIME OR FREQUENCY OF PUBLICATION

After acceptance by the LAWtrust PA, the LAWtrust Root CA 2048 CPS shall be published in the manner described in **Error! Reference source not found.**.

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.

2.4 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

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. The common name shall be the name associated with LAWtrust.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The subject name contained in certificates issued under the LAWtrust PKI Hierarchy must be meaningful in the sense that the LAWtrust Root CA 2048 is provided with proper evidence of the association existing between the name and the entity to which it belongs.

The Distinguished name (DN) of certificates and CRLs issued under the LAWtrust Root CA 2048 shall have the Issuer field of set to the following (LDAP Notation):

CN= LAWtrust Root Certification Authority 2048, O=LAWtrust, C=ZA

The DN (LDAP Notation) in the Subject field of the Sub-CA certificates that are issued will be:

CN= LAWtrust AeSign Certification Authority 2048, O=LAWtrust, C=ZA

CN=LAWtrust AeSign CA02, O=LAWtrust, C=ZA

CN=LAWtrust AATL CA01, O=LAWtrust, C=ZA

The common name in the Subscriber DN will represent the Subscriber (in this case the Sub-CAs) in a way that is easily understandable for humans. The certificate types supported by the LAWtrust Root CA 2048 are covered in Appendix-B of this document.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The LAWtrust Root CA 2048 may not issue anonymous or pseudonymous certificates.

3.1.4 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.

LAWtrust Root CA 2048 shall only use Uniform Resource Indicators (URIs) in accordance with the applicable Internet Engineering Task Force (IETF) standards. Subject Alternative Name forms are interpreted in accordance with applicable ISO and IETF Standards. The following table provides the rules for interpreting the various name forms.

Name Form	Standard
DN	X.500
URL	RFC-1738
Internet e-mail address	RFC-822
DNS	RFC-1034

3.1.5 Uniqueness of Names

All distinguished names shall be unique across the LAWtrust Root CA 2048. Names shall not be re-used for another Sub-CA. After a Sub-CA certificate expires or is revoked, the name can be re-used to re-issue a certificate to the same Sub-CA.

The LAWtrust Root CA 2048 will be configured in such a manner as to enforce name uniqueness for certificates that it issues. The LAWtrust Root CA 2048 is responsible for ensuring name uniqueness in Sub-CA certificates issued by it. Additional naming attributes for uniquely identifying the subject include serial number, etc.

3.1.6 Recognition, Authentication and Role of Trademarks

No Stipulation

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

LAWtrust maintains 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 Authentication of Issuer Identity

The LAWtrust Root CA 2048 operates under the LAWtrust PKI and as such complies with the requirements as set forth by LAWtrust. The LAWtrust Root CA 2048 does not issue certificates to other entities other than its own Subordinate Issuing CAs.

3.2.3 Identity-Proofing of Individual Identity

3.2.3.1 Identity-Proofing of End User Subscribers

No stipulation. The LAWtrust Root CA 2048 does not issue certificates to end users

3.2.3.2 Identity-Proofing of Device Subscribers

No stipulation.

3.2.3.3 Identity-Proofing of Organizational Entities

No Stipulation.

3.2.4 Non-verified Subscriber Information

No Stipulation.

3.2.5 Validation of Authority

LAWtrust Security Committee shall verify the rights conferred to the applicant of a Subordinate Issuing CA to request a certificate. The approval together with a form of identity shall be verified as part of the Key Ceremony process.

3.2.6 Criteria of Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The usage periods for the Sub-CA private keys are described in section 6.3.2. During the Re-keying process the LAWtrust Root CA 2048 will create a new certificate with the same characteristics as the old certificate but with a new and different key pair and serial number. This new certificate may be given a new validity period or use the validity period that appeared in the old certificate.

The authentication of a Routine Re-key shall follow the same procedure as the initial certificate issuance. This shall be performed as part of a scripted Key Ceremony.

3.3.2 Identification and Authentication for Re-key After Revocation

Where the information contained in a Sub-CA certificate has changed or there is a known or suspected compromise of the private key, the LAWtrust Root CA 2048 must authenticate a re-key in the same manner as for initial registration. A Key Ceremony process shall be constituted and followed to generate new keys for the revoked Sub-CA certificate.

3.4 Identification and Authentication for Revocation Requests

Prior to the revocation of a Sub-CA certificate, the LAWtrust Security Committee shall verify that the revocation has been requested by an authorized person.

Acceptable procedures for authenticating the revocation requests include:

- A request for revocation of a Sub-CA is initiated by an authorized person within LAWtrust, such as the Policy Authority;
- The LAWtrust Security Committee shall approve such requests
- Revocation of the Sub-CA shall be performed using a scripted and witnessed process.

4 Certificate Life-Cycle Operational Requirements

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

4.1 Certificate Application

The LAWtrust Security Committee shall consider applications for Sub-CA certificate generation as part of a new CA establishment. LAWtrust Security Committee shall only accept applications for Sub-CA establishment from Trusted employees within LAWtrust.

The LAWtrust Security Committee shall perform the following steps when an application for a new certificate is received:

- Establish the applicant's authorization to request the establishment of a CA;
- Establish and record the identity of the applicant;
- Verify the existence of a signed request to establish the Sub-CA.
- Approve the Key generation Script and set the date for the Key Ceremony

The LAWtrust Root CA 2048 will perform the following after approval by the LAWtrust Security Committee:

- Constitute the Key Shareholders and relevant parties for the LAWtrust Root CA 2048;
- Activate the LAWtrust Root CA 2048 key;
- Generate the Certificate relating to that Sub-CA; and
- Transmits the Certificate to the requesting Sub-CA.
- Publish the Sub-CA key to the repository

4.1.1 Submission of Certificate Application

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 Enrollment Process and Responsibilities

4.1.2.1 Issuing CAs

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 Application Processing

4.2.1 Performing Identity-proofing 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 Applications

This is an internal process to LAWtrust.

4.2.3 Time to Process Certificate Applications

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 Certificate Issuance

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 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/repository)

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 SUB-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.

4.5.2 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

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different private key.

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

4.7.1 Circumstances for Certificate Re-key

Prior to the expiration of an existing Sub-CA Certificate, it is necessary for the Sub-CA to update the certificate to maintain continuity of Certificate usage.

Manual Certificate re-key may be performed within or after one-month of certificate expiry.

The process for rekeying a Sub-CA certificate shall be done as part of a witnessed key ceremony process similar to the initial key generation and certificate issuance

4.7.2 Who can Request a Certificate Re-key

Certificate re-key may be requested by an authorized LAWtrust representative. The requestor's identification shall be determined and verified by the LAWtrust Security Committee.

4.7.3 Processing Certificate Re-keying Requests

Processing of Sub-CA certificate re-keying request shall be initiated only after successful verification of the re-key request from LAWtrust authorized representative; In each case the LAWtrust Security Committee shall approve all re-key requests.

4.7.4 Notification of Re-Keyed Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to Relying Parties shall follow the same procedures as notification for newly issued Sub-CA certificates.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is in accordance with section 4.4.1 of this CPS.

4.7.6 Publication of the Re-keyed Certificate by the CA

The re-keyed certificate is published in the appropriate repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Generally, LAWtrust Root CA 2048 does not notify other entities of a re-keyed certificate apart from the requesting LAWtrust representative.

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 Circumstance for Revocation of a Certificate

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 of a Certificate

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.

4.9.3.1 Procedure for Requesting the Revocation of a Sub-CA Certificate

A CA requesting revocation of its CA Certificate is required to communicate the request to the LAWtrust Policy Authority (PA). The LAWtrust PA shall seek approval from the LAWtrust Security Committee, which will then authorize the revocation of the Sub-CA certificate. The LAWtrust PA may also initiate the Sub-CA certificate revocation if it deems necessary. The revoked CA certificate shall be published in the CRL of the LAWtrust Root CA 2048.

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 Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

The LAWtrust Root CA 2048 will publish its CRLs at least once every 6 months and within 24 hours of any Certificate revocation of its Sub-CAs.

4.9.8 Maximum Latency of CRLs

CRLs shall be published in the Repositories within 24 hours of Certificate revocation.

4.9.9 Online Revocation 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.

4.9.10 Online Revocation Checking Requirements

No stipulation.

4.9.11 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.

4.9.12 Special Requirements Related To 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.

4.9.13 Circumstances for Certificate 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.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.9.17 Circumstances for Terminating Suspended Certificates

No stipulation.

4.9.18 Procedure for Terminating the Suspension of a Certificate

No stipulation.

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 CRLs from time to time to ensure the availability of service for parties relying on the CRL.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

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 SECURITY CONTROLS

LAWtrust operates the LAWtrust PKI (LAWtrust Root CA 2048, LAWtrust Root CA2 (4096) and Issuing CAs), Repositories and OCSP responder at the LAWtrust data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. LAWtrust limits access to functions critical to registration and certificate to personnel in Trusted Roles.

The LAWtrust PKI shall have physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

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 POWER AND AIR CONDITIONING

LAWtrust Data Center has a UPS and back-up electrical generators and sufficient back-up capability to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

The design of LAWtrust PKI facilities ensures that no single point of failure is supported by providing the following measures:

- Two independent power supplies feeding the LAWtrust Data Centre;

- Uninterruptible Power Supply units and stand-by generators for the entire building; and
- Switchover of the services to a backup facility in the case of an emergency or disaster as per LAWtrust Business Continuity Plan.

A fully redundant air-conditioning system is installed in the PKI areas.

5.1.4 Water Exposure

The hosted data centre is protected against water exposure.

5.1.5 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.

5.1.6 Media Storage

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

5.1.7 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.

5.1.8 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

5.3.1 BACKGROUND, QUALIFICATIONS AND EXPERIENCE REQUIREMENTS

All persons filling trusted roles are selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the LAWtrust Trusted Roles document and LAWtrust Organization Structure document.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

LAWtrust conducts background investigations for all LAWtrust personnel including trusted roles and management positions. Background check shall take into account the following:

- Availability of satisfactory character reference, i.e. one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles.

5.3.3 Training Requirements And Procedures

LAWtrust will provide proper training to all personnel performing duties with respect to the operation of the LAWtrust PKI, Repositories and OCSP Responder. Training shall cover the following aspects:

- PKI and Information Security concepts;
- All PKI software versions in use on the LAWtrust PKI, Repositories and OCSP Responder systems;
- All LAWtrust PKI duties that the personnel are expected to perform on LAWtrust Root CA 2048;
- Disaster recovery and business continuity procedures; and
- The meaning and effect of the LAWtrust CP and this CPS.

Documentation of all personnel who received training and the level of training completed shall be maintained by LAWtrust.

5.3.4 Retraining Frequency and Requirements

Individuals performing PKI roles are made aware of changes in the LAWtrust PKI operation. Any significant change to the operations will necessitate a training awareness plan, and the execution of such plan is documented. Examples of such changes are LAWtrust PKI software or hardware upgrade, changes in automated security systems, and relocation of equipment.

The LAWtrust Root CA 2048 shall review and update its training program at least once a year to accommodate changes in the LAWtrust *PKI* system

5.3.5 Job Rotation Frequency and Sequence

The LAWtrust Root CA 2048 shall ensure that any change in the staff complement will not affect the operational effectiveness of the PKI services and security thereof.

5.3.6 Sanctions for Unauthorized Actions

The LAWtrust Root CA 2048 shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions not permitted by the CP, CPS and/or other LAWtrust Root CA 2048 operational procedures.

5.3.7 Contracting Personnel Requirements

When LAWtrust uses a contractor to perform services, there will be adequate procedures with explicitly stated objectives and supervision will be in place to ensure that any tasks performed in accordance with the LAWtrust CP, this CPS, LAWtrust PKI Policies as well as the

requirements stipulated in the contractor's contract of employment. Contractor personnel shall be subject to the same sanctions as other personnel as set forth in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

LAWtrust provides sufficient documentation to its personnel in order for them to perform their job responsibilities competently and satisfactorily.

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.

5.4.1 Types of Events Recorded

The LAWtrust PA shall ensure recording in audit log files all events relating to the security of the CA system hosted in LAWtrust data centre. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events.
2. Issuing CA Certificate lifecycle management events, including:
   a. Certificate requests, renewal, and re-key requests, and revocation;
   b. All verification activities stipulated in these Requirements and the Issuing CA's Certification Practice Statement;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Acceptance and rejection of certificate requests;
   e. Issuance of Certificates; and
   f. Generation of Certificate Revocation Lists.
3. Security events, including:

a. Successful and unsuccessful PKI system access attempts;
b. PKI and security system actions performed;
c. Security profile changes;
d. System crashes, hardware failures, and other anomalies;
e. Firewall and router activities; and
f. Entries to and exits from the LAWtrust PKI facility.

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 Frequency of Processing Data

Audit logs are required to be processed in accordance with LAWtrust Audit and Compliance Policy.

5.4.3 Retention Period for Audit LOG

The LAWtrust Root CA 2048 shall retain all system generated (electronic and manual) audit records onsite for a period not less than twelve (12) months from the date of creation.

5.4.4 Protection of Security Audit Data

Read access to the journal information is granted to personnel requiring this access as part of their duties. Only authorized roles can obtain access.

The journal is stored in the text files and access to this is protected against unauthorized access by the CA application and through special security measures on the operating system level.

5.4.5 Audit LOG Backup Procedures

The journal is an integral part of the CA database and is therefore part of the daily backup. The entire database is encrypted on the disk as well as on the backup media.

Audit log backup procedures are in accordance with LAWtrust Audit and Compliance Policy.

5.4.6 Audit Collection System (Internal or External)

The audit log or journal is an integral part of the CA software. The audit system ensures the integrity of the audit data being collected. In case of the audit system stopping to function, the LAWtrust Root CA 2048 shall determine whether to suspend or continue with operations.

5.4.7 Notification to Event-Causing Subject

Event-causing subject are not notified.

5.4.8 Vulnerability Assessments

LAWtrust performs routine assessments of security controls. This self-assessment includes periodic review of error logs on systems, storage of assets and records, security audit data for alerts or irregularities, alarm logs, access logs, incident reports, and audit log analysis.

Apart from this, LAWtrust data centre is constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed.

LAWtrust performs third party penetration testing for LAWtrust data centre infrastructure at least once a year and doing regular vulnerability assessment internally. Also Risk Assessment is performed at least once a year as per LAWtrust Risk Assessment Methodology. LAWtrust Risk Assessment exercise includes identification of foreseeable internal and external threats,

assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems, technology.

Based on the Risk Assessment exercise, the LAWtrust Root CA 2048 shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

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.

5.5.1 Types of Events Archived

The LAWtrust Root CA 2048 archives records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. The LAWtrust Root CA 2048 shall make these audit logs available to its Qualified Auditor upon request.

a) Audit logs generated by the PKI CA software;
b) RA and other agreements;
c) Records pertaining to identification and authentication information;
d) Physical access logs;
e) System configuration changes and maintenance;
f) CA personnel changes;
g) Discrepancy and No compromise reports;
h) Information concerning the destruction of sensitive information;
i) Current and past versions of all Certificate Policies;
j) Current and past versions of Certification Practice Statements;
k) Vulnerability Assessment Reports;
l) Threat and Risk Assessment Reports;
m) Compliance Inspection Reports;
n) Documents identifying all personnel who received CA related training and the level of training completed; and

o) The LAWtrust Root CA 2048 shall archive any necessary keys and passwords for a period of time sufficient to support the functionalities.

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by the LAWtrust PA. LAWtrust's minimum retention period for archive data is established at 7 years.

The LAWtrust Root CA 2048 shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

Applications needed to process the archive data shall also be maintained for the archival retention period.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by LAWtrust, LAWtrust PA, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4 Archive Backup Procedures

Only one copy of the archive is maintained. In other words, archive itself is not backed up.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information obtained from the Time Server.

System logs are automatically time stamped and systems use a dedicated time server to maintain synchronized time.

5.5.6 Archive Collection System (Internal or External)

The type of Archive Collection System, whether internal or external, is specified in LAWtrust Archival Policy.

5.5.7 Procedures to Obtain and Verify Archive Information

Information on how the archive information is created, verified, packaged, transmitted and stored is detailed in the LAWtrust Archival Policy. These policies and procedures are updated and augmented to reflect the legal and best practice requirements for managing and protecting electronic records.

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 CA Termination

5.8.1 CA 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.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

The signing key pair for the LAWtrust Root CA 2048 was created during the initial startup 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.

6.1.2 PRIVATE KEY DELIVERY TO END-ENTITIES

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

6.1.3 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.

6.1.4 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]*.

6.1.5 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.

6.1.6 Public Key Parameters Generation and Quality Checking

The LAWtrust Root CA 2048 shall generate public keys in accordance with industry standards such as FIPS 186 and check public key parameters for their validity.

6.1.7 Key Usage Purposes

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.

6.2 Private Key Protection and Crypto-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.

6.2.1 Cryptographic Module Standards and Controls

See section 6.1.1 of this CPS for the description of the cryptographic modules.

6.2.2 CA Private Key Multi-Person Control

Multi-person control of the LAWtrust Root CA 2048 private key is achieved using an "m-of-n" split key knowledge scheme. LAWtrust Root CA 2048 keys can only be accessed on the physical and logical level by adhering to '3 out of 12' control, meaning that 3 of the 12 persons are present.

6.2.3 Private Key Escrow

See section 4.12 of this document.

6.2.4 Private Key Backup

LAWtrust uses the mechanisms provided by the HSM's to backup the LAWtrust Root CA 2048 signing key. A second copy may be kept at the CA backup location identified as business continuity location. A third copy may be kept at the CA backup location identified as disaster recovery location. Procedures for LAWtrust Root CA 2048 signing Private Key backup are

detailed in LAWtrust PKI Backup and Restore Procedures. The CA signing key is backed up under the same multi-person control as the original signature keys.

6.2.5 Private Key Archival

The LAWtrust Root CA 2048 does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The LAWtrust Root CA 2048 shall generate, activate and store private keys in FIPS 140-2 Level 3 or above rated Hardware Cryptographic Modules. When the Private Keys are outside the HSM, they shall be kept in encrypted form.

LAWtrust Root CA 2048 keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

6.2.7 Private Key Storage on Cryptographic Module

The LAWtrust Root CA 2048's private keys are stored on FIPS 140-2 Level 3 validated modules in encrypted form.

6.2.8 Method of Activating Private Keys

The LAWtrust Root CA 2048's private key shall be activated by a threshold number of Shareholders, as defined in LAWtrust Operations Policies and Procedures, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process. A deactivated key shall be kept encrypted or otherwise secured within the cryptographic module, to prevent unauthorized access.

6.2.9 Methods of Deactivating Private Keys

The LAWtrust Root CA 2048's private keys shall be deactivated by a threshold number of shareholders, as defined in LAWtrust Operations Policies and Procedures, by removing their secure media.

6.2.10 Methods of Destroying Private Keys

The LAWtrust Root CA 2048 and Sub-CAs under the PKI hierarchy Private keys shall be destroyed as per LAWtrust Cryptographic Devices Lifecycle Management Policy and Procedure, which shall be consistent with section 6.2.2 of the LAWtrust CP.

6.2.11 Cryptographic Module Rating

The CA private keys are stored on FIPS 140-2 Level 3 validated Hardware Security Modules.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archive

The LAWtrust Root CA 2048 certificate (which contains the public key) is backed up and archived as part of the LAWtrust Root CA 2048 and LAWtrust data centre routine backup procedures.

6.3.2 Certificate Operational Periods and Key Usage Periods

The table below details key usage, length and certificate lifetime for the corresponding keys:

Key/Certificate	Key Length in Bits	Maximum Validity Period
LAWtrust Root CA 2048 signing key and certificate	2048	118 months
LAWtrust AeSign Certification Authority 2048 Signing Key and Certificate	2048	118 months
LAWtrust AeSign CA02 Signing Key and Certificate	2048	118 months
LAWtrust AATL CA01 Signing Key and Certificate	2048	118 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The LAWtrust Root CA 2048 and Sub-CA cryptographic module activation data will be generated locally at the time of key generation by personnel in the trusted role and responsible for controlling the activation data.

6.4.2 Activation Data Protection

If written down CA cryptographic module activation data is placed into secure packages which are then stored within secure containers in a highly secured environment inside LAWtrust data centre.

In addition, the activation data shall be secured at the same level as the cryptographic data for the LAWtrust Root CA 2048 and Sub-CAs. Such data shall be stored under multi-person control and shall not be stored with the cryptographic modules (HSMs).

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

The server on which the LAWtrust Root CA 2048 operates is offline and physically secured as described in **Error! Reference source not found.** 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 **Error! Reference source not found.**

6.5.1 Specific Computer Security Technical Requirements

The LAWtrust Root CA 2048 servers hosted in LAWtrust data centre are protected by external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. Access to the system for System Administrators is granted only over secure and restricted protocols using strong public-key authentication.

LAWtrust data centre has implemented layered security approach to ensure the security and integrity of the computers used to run the LAWtrust Root CA 2048 software. The following controls ensure the security of LAWtrust data centre operated computer systems:

- Hardened operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;

- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Security 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.

6.6.1 System Development Controls

LAWtrust employs the following System Development controls:

- LAWtrust may use standard software from product vendors for version control. Where LAWtrust uses its own software products, these have been developed using documented software development processes;
- Hardware and software procured to operate the CA is purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device);
- CA hardware and software configurations are dedicated to performing one task: the CA. No other applications, hardware devices, network connections, or component software that is not part of the CA operation will be installed;
- LAWtrust undertakes all reasonable precautions to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA are procured. The CA hardware and software is scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased in the same manner as original equipment, and are installed by trusted and trained personnel according to policies and procedures established in LAWtrust's Operations Policies and Procedures.

6.6.2 Security Management Controls

System security management shall be controlled by the privileges assigned to system accounts and by the trusted roles described in section 5.2.1, according to appropriate standards (e.g. ISO/IEC 27001:2013 or similar).

The configuration of the LAWtrust Root CA 2048 system as well as any modifications and upgrades must be documented and controlled in accordance with LAWtrust Change Management Policy. A formal configuration management methodology must be used for installation, ongoing maintenance and evolution of the CA system. No upgrades shall be permitted without prior offline testing and assessment, and regular backups must be taken.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The Repository and CRL infrastructure will be connected to the internet in such a way so as to provide continuous service to Relying Parties. Redundancy is provided through the Repository and network infrastructure to prevent loss of service even during maintenance and backup procedures.

LAWtrust data centre uses network design of multiple security layers making use of several security technologies including firewalls, intrusion prevention systems, anti-virus, anti-spyware software to protect network access to on-line LAWtrust Root CA 2048's and Repository equipment. These technologies may limit the services allowed to and from the on-line CA's, Repository and OCSP Responder equipment to those authorized to have such access.

LAWtrust data centre network security controls are designed to protect LAWtrust infrastructure against network attacks. All unused network ports and services are turned off. These network security controls include effective firewall management, including port restrictions and IP address filtering.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 Time Stamping

Certificates, CRLs, and other revocation database entries contain time and date information. System logs are automatically time stamped and systems use a dedicated time server to maintain synchronized time.

Time derived from the time service shall be used for establishing the time of:

- Initial validity time of the Sub-CA Certificates;
- Revocation of Sub-CA Certificates;
- Posting of CRL updates;

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions. The detailed Certificate profile for the LAWtrust Root CA 2048 is described in the LAWtrust PKI Certificate Profiles document, an internal LAWtrust Operational document.

7.1.1 VERSION NUMBERS

LAWtrust Root CA 2048 shall issue X.509 v3 certificates.

7.1.2 CERTIFICATE EXTENSIONS

LAWtrust Root CA 2048 and its critical private extensions shall be interoperable in their intended community of use.

Subordinate certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by LAWtrust CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

LAWtrust Root CA 2048 shall sign Subordinate Certificates using any one of the following:

sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

sha384WithRSAEncryption algorithm (1.2.840.113549.1.1.12).

ecdsawithsha256 algorithm (1.2.840.10045.4.3.2).

ecdsawithsha384 algorithm (1.2.840.10045.4.3.3).

ecdsawithsha512 algorithm (1.2.840.10045.4.3.4).

The algorithm identifier of the subject Public Key shall be:

rsaEncryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 Name Forms

Certificates issued by LAWtrust Root CA 2048 contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 Name Constraints

No Stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CPS shall assert a certificate policy OID.

7.1.7 Usage of Policy Constraints Extension

No Stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL Profile

The LAWtrust Root CA 2048 CRL Profile is shown below:

7.2.1 LAWtrust Root CA 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 Root 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

7.2.2 Version Numbers

The LAWtrust Root CA 2048 shall issue X.509 version two (v2) CRLs.

7.2.3 CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use.

7.3 OCSP Profile

No Stipulation.

7.3.1 Version Number

No Stipulation.

7.3.2 OCSP Extensions

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 of Audit or Assessments

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 and 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 Financial Responsibility

LAWtrust Root CA 2048 disclaims all liability implicit or explicit due to the use of any certificates issued by the LAWtrust Issuing CAs which certify public keys of subscribers.

9.2.1 Insurance Coverage

LAWtrust Root CA 2048 shall hold insurance cover in lieu of its performance and obligations under guidelines deemed sufficient by the LAWtrust Root CA 2048.

9.2.2 Other Assets

LAWtrust Root CA 2048 shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 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.

9.3.1 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 9.3.1.1 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.

9.3.1.1 Registration Information

All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed CA Agreements;
- Any information requested by LAWtrust when it receives an application from a third party to operate as a CA or a Cross-Certified CA;
- Any corporate or personal information held by LAWtrust or LAWtrust Root CA 2048 related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfill the requirements of LAWtrust CP, and in accordance with LAWtrust Privacy Policy.

9.3.1.2 Certificate Information

The reasons for a certificate being suspended or revoked is considered confidential information, with the sole exception of the revocation of the LAWtrust Root CA 2048 due to:

- The compromise of their private key, in which case a disclosure may be made that the private key has been compromised; or
- The termination of the LAWtrust Root CA 2048 in which case prior disclosure of the termination may be given.

9.3.1.3 PKI Documentation

LAWtrust Document Control Policy specifies which documents are considered to be confidential.

9.3.2 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.

9.3.3 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.

9.4 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]*.

9.4.1 Privacy Plan

All personally identifying information as defined by LAWtrust Privacy Policy shall be protected from unauthorized disclosure.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3 Information not Deemed Private

Information appearing in Subordinate Certificates such as the organization name, and public key will not be deemed private. LAWtrust Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 Responsibility to Protect Private Information

Access to LAWtrust Root CA 2048 held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5 Notice and Consent to Use Private Information

Requirements for notice and consent to use private information are defined in the respective Agreements and LAWtrust Privacy Policy.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with LAWtrust Privacy Policy.

9.4.7 Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with LAWtrust Privacy Policy.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among LAWtrust participants are governed by the applicable agreements.

The LAWtrust PA retains exclusive rights to any products or information developed under or pursuant to LAWtrust CP.

9.6 Representations and Warranties

9.6.1 LAWtrust Root CA 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.

9.6.2 RA Representations and Warranties

The same liability provisions that apply in Section 9.6.1 with respect to LAWtrust Root CA 2048 shall apply with respect to LAWtrust OA and employees, and directors of the foregoing.

9.6.3 Relying Parties 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.

9.6.4 Subscriber Representations and Warranties

No stipulation.

9.7 Disclaimers of Warranties

Except as specifically provided in sections **Error! Reference source not found.** 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.

9.8 Limitations 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.

9.9 Indemnities

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend,

indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

The RAs shall indemnify, defend and hold harmless the following parties:

- LAWtrust, its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- The RA's own employees, arising from any of the RA's operations and activities as a RA, of any entity or services subordinated or outsourced by the RA; and
- Any parties relying on the RA's Certificates or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CPS shall be effective upon approval by the LAWtrust Security Committee. LAWtrust shall be notified of all changes to this document. Once the CPS becomes effective it is published in the repository. Amendments to this CPS upon approval become effective and replace the older version in the repository.

9.10.2 TERMINATION

This CPS as amended from time to time shall remain in force until it is replaced by a new version. The latest version of the LAWtrust Root CA 2048 CPS can be found at: *[https://www.lawtrust.co.za/repository]*

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CPS, all LAWtrust Root CA 2048 participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

All communication between LAWtrust, LAWtrust PA and LAWtrust Root CA 2048 shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting the corresponding Issuing CA's Certificate assurance level.

9.12 Amendments

9.12.1 Procedure for Amendment

The LAWtrust PA shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be communicated to the LAWtrust PA. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the LAWtrust Root CA 2048 shall be managed as per the LAWtrust Change Management Policy.

LAWtrust Root CA 2048 reserves the right to change this CPS from time to time. LAWtrust Root CA 2048 will incorporate any such change into a new version of this CPS and, upon approval, publish the new version. The new CPS will carry a new version number.

9.12.2 Notification Mechanism and Period

The LAWtrust PA reserves the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the Saudi PKI participants and other parties designated by the LAWtrust PA shall provide their comments to the LAWtrust PA in accordance with LAWtrust rules.

The LAWtrust PA's decision to designate amendments as material or non-material shall be at the PA's sole discretion.

Any changes to this CPS shall be made available within two weeks of approval by LAWtrust PA.

9.12.3 Circumstances under which OID must be changed

The policy OID shall only change if the change in the CPS results in a material change to the trust by the relying parties, as determined by the LAWtrust PA.

9.13 Dispute Resolution Procedures

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.

DISPUTE RESOLUTION COMMITTEE

The LAWtrust PKI Dispute Resolution Committee will arbitrate on all claims or disputes arising out of or related to the operation of LAWtrust CAs.

DISPUTE RESOLUTION POLICY

LAWtrust PKI Dispute Resolution Policy is applicable to all participants of the LAWtrust PKI.

9.14 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.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to national, state, local and foreign laws, rules and regulation, ordinances, decrees and orders including but not limited to, restrictions on exporting or importing software, hardware or technical information.

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 ASSIGNMENT

Except where specified by other contracts, no party may assign or delegate any of its rights or duties under the LAWtrust Root CA 2048 CPS, without the prior written consent of the LAWtrust PA.

9.16.3 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.

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

This document shall be treated according to laws of South Africa. Legal disputes arising from the operation of the LAWtrust Root CA 2048 will be treated according to the laws of the South Africa.

9.16.5 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.

9.17 Other Provisions

9.17.1 Fiduciary Relationships

Nothing contained in this CPS shall be deemed to constitute either the LAWtrust Root CA 2048, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the LAWtrust Root CA 2048 and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CPS or any Agreement between a third party and a Relying Party shall confer on any Customer, Relying Party, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the LAWtrust Root CA 2048.

9.17.2 Administrative Processes

As specified in LAWtrust Operations Policies and applicable Agreements.

APPENDIX -A: 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)
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.

Term	Definition
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.
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, (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

Term	Definition
	the subscriber's public key; and (ii) the message has been altered since the transformation was made.
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 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,

Term	Definition
	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.
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
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.

Term	Definition
Registration Authority 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.
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.
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 control the implementation of information security as a whole within LAWtrust.

Term	Definition
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.
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.

APPENDIX-B: CERTIFICATE TYPES & POLICIES

B.1 CERTIFICATE TYPES SUPPORTED

B.1.1 LAWTRUST ROOT CA 2048 CERTIFICATE

B.1.1.1 LAWtrust Root CA 2048 Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	LAWtrust Certificate Policy
2	Policy OID	**1.3.6.1.4.1.54383.1.1**
3	Subject	"CN = LAWtrust Root Certification Authority 2048, O = LAWtrust, C = ZA"
4	Application Usage	LAWtrust Root CA 2048 Certificates are CA Certificates and are not tied to any specific application or function. The applications using the LAWtrust Root CA 2048 issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The LAWtrust Root CA 2048 Certificate is used to sign Subordinate CA certificates and CRLs.
5	Verification Process	The process of verifying the LAWtrust Root CA 2048 certificate request is done as part of the Key Ceremony Process
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. LAWtrust Root CA 2048 KeyPairs shall be generated using Hardware Security Modules meeting the stipulated FIPS 140-2 level.
7	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the LAWtrust OA who shall in turn sign the request. The signed certificate shall be returned to LAWtrust to complete the process of CA configuration
8	Key Usage	The LAWtrust Root CA 2048 certificate and keys shall be used to sign Sub CA certificates and CRLs only

S. No.	Attribute	CA Certificate
9	Private Key Protection	The LAWtrust Root CA 2048 Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 118 months (9 years, 10 months)
11	Key Backup	The LAWtrust Root CA 2048 shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	The LAWtrust Root CA 2048 Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

B.1.2 LAWTRUST AESIGN CERTIFICATION AUTHORITY 2048 CERTIFICATE

This is the Subordinate Issuing CA certificate that is issued by the LAWtrust Root CA 2048.

B.1.2.1 LAWtrust AeSign Certification Authority 2048 Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	LAWtrust Certificate Policy
2	Policy OID	**1.3.6.1.4.1.54383.1.1.1**
3	Subject	"CN=LAWtrust AeSign Certification Authority 2048, O = LAWtrust, C =ZA"
4	Application Usage	LAWtrust AeSign Certification Authority 2048 Certificates are CA Certificates and are not tied to any specific application or function. The applications using the LAWtrust AeSign Certification Authority 2048 issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The LAWtrust AeSign Certification Authority 2048 Certificate is used to sign end entity subscriber certificates and CRLs.

5	Verification Process	The process of verifying the LAWtrust AeSign Certification Authority 2048 certificate request is done as part of the Key Ceremony Process
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. LAWtrust AeSign Certification Authority 2048 Key Pairs shall be generated using Hardware Security Modules meeting the stipulated FIPS 140-2 level.
7	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the LAWtrust Root CA 2048 that shall in turn sign the request. The signed certificate shall be returned to complete the process of the LAWtrust AeSign Certification Authority 2048 configuration
8	Key Usage	The LAWtrust AeSign Certification Authority 2048 certificate and keys shall be used to sign end entity subscriber certificates and CRLs only
9	Private Key Protection	The LAWtrust AeSign Certification Authority 2048 Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 60 months (5 years)
11	Key Backup	The LAWtrust AeSign Certification Authority 2048 shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	The LAWtrust AeSign Certification Authority 2048 Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

B.1.3 LAWTRUST AESIGN CA02 CERTIFICATE

This is the Subordinate Issuing CA certificate that is issued by the LAWtrust Root CA 2048.

B.1.3.1 LAWtrust AeSign CA02 Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	LAWtrust Certificate Policy
2	Policy OID	**1.3.6.1.4.1.54383.1.1.2**
3	Subject	"CN=LAWtrust AeSign CA02, O = LAWtrust, C = ZA"
4	Application Usage	LAWtrust AeSign CA02 Certificates are CA Certificates and are not tied to any specific application or function. The applications using the LAWtrust AeSign CA02 issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The LAWtrust AeSign CA02 Certificate is used to sign end entity subscriber certificates and CRLs.
5	Verification Process	The process of verifying the LAWtrust AeSign CA02 certificate request is done as part of the Key Ceremony Process
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. LAWtrust AeSign CA02 Key Pairs shall be generated using Hardware Security Modules meeting the stipulated FIPS 140-2 level.
7	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the LAWtrust Root CA 2048 that shall in turn sign the request. The signed certificate shall be returned to complete the process of the LAWtrust AeSign CA02 configuration
8	Key Usage	The LAWtrust AeSign CA02 certificate and keys shall be used to sign end entity subscriber certificates and CRLs only
9	Private Key Protection	The LAWtrust AeSign CA02 Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 60 months (5 years)

11	Key Backup	The LAWtrust AeSign CA02 shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	The LAWtrust AeSign CA02 Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

B.1.4 LAWTRUST AATL CA01 CERTIFICATE

This is the Subordinate Issuing CA certificate that is issued by the LAWtrust Root CA 2048.

B.1.3.1 LAWtrust AeSign CA02 Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	LAWtrust Certificate Policy
2	Policy OID	**1.3.6.1.4.1.54383.1.1.3**
3	Subject	"CN= LAWtrust AATL CA01, O = LAWtrust, C = ZA"
4	Application Usage	LAWtrust AATL CA01 Certificates are CA Certificates and are not tied to any specific application or function. The applications using the LAWtrust AATL CA01 issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The LAWtrust AATL CA01 Certificate is used to sign end entity subscriber certificates and CRLs.
5	Verification Process	The process of verifying the LAWtrust AATL CA01 certificate request is done as part of the Key Ceremony Process

6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. LAWtrust AATL CA01 Key Pairs shall be generated using Hardware Security Modules meeting the stipulated FIPS 140-2 level.
7	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the LAWtrust AATL CA01 that shall in turn sign the request. The signed certificate shall be returned to complete the process of the LAWtrust AATL CA01 configuration
8	Key Usage	The LAWtrust AATL CA01 certificate and keys shall be used to sign end entity subscriber certificates and CRLs only
9	Private Key Protection	The LAWtrust AATL CA01 Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 60 months (5 years)
11	Key Backup	The LAWtrust AATL CA01 shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	The LAWtrust AATL CA01 Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

10 SIGN OFF ACCEPTANCE

Name:	Katekani Hlabathi
Authority:	Policy Authority
Title:	Chief Information Officer
Date:	2021-08-06
Signature: