www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CPS_AES_CA_V013 2026-08-18
	Location	https://www.lawtrust.co.za/repository
	Version	V013 2026-08-18
	Policy Authority	LAWtrust PA

LAWTRUST AESIGN CERTIFICATION AUTHORITY 2048

Certification Practice Statement

(LAWtrust AeSign Certificate Authority 2048 CPS)

Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07

("LAWtrust")

20 Woodlands Drive,

Woodlands Office Park, Woodmead,

Johannesburg, South Africa

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

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
V001 2015-11-01	2015-11-01	Bruce Anderson	Initial publication with amendments for SHA2	Expired
V002 2016-11-01	2016-11-01	Bruce Anderson	2016 Review, new format	Expired
V003 2017-05-11	2017-05-11	Bruce Anderson	Included various housekeeping items. Included the use of SSCD Corrected invalid links	Expired
V004 2017-10-19	2017-10-19	Bruce Anderson	2017 review	Expired
V005 2018-12-12	2018-12-12	Eduard Oosthuizen	QA Review, apply new document template, 2018 Review	Expired
V006 2021-08-31	2021-08-31	Marcile De Waal Katekani Hlabathi	Updated the CPS to conform to RFC3647 Standard. Add Mozilla requirements on email validation	Expired
V007 2022-10-31	2022-10-31	Marcile De Waal	Yearly review	Expired
V008 2023-09-01	2023-10-31	Marcile De Waal	Yearly Review	Expired
V009 2024-08-14	2024-10-31	Marcile De Waal	Yearly Review	Expired
V010 2025-03-10	2025-03-10	Marcile De Waal	Policy Changes	Expired
V011 2025-08-10	2025-10-31	Marcile De Waal	Yearly Review	Expired
V012 2026-02-25	2026-02-27	Marcile De Waal	Addition to allow for system authentication certs.	Expired
V013 2026-08-18	2026-10-31	Marcile De Waal	Yearly Review	Operational

Document references

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

Ref.	Document Title	File Location
1	LAWtrust Certificate Policy	LAWtrust Internal Policy (Level 2)
2	LAWtrust AeSign Certificate Authority RA Charter	https://www.lawtrust.co.za/repository
3	LAWtrust Relying Party Agreement	https://www.lawtrust.co.za/repository
4	LAWtrust Subscriber Agreement	https://www.lawtrust.co.za/repository
5	LAWtrust Privacy Policy	https://www.altron.com/policies/privacy-policy/
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 7

1.1 Overview 7

1.2 Document Name and Identification 9

1.3 PKI participants 9

1.4 Certificate Usage 12

1.5 Policy Administration 13

1.6 Definitions and Acronyms 14

2. Publication and Repository Responsibilities 14

2.1 Repositories 14

2.2 Publication of Certification Information 16

2.3 Time or Frequency of Publication 18

2.4 Access Controls on Repositories 18

3. Identification and Authentication 18

3.1 Naming 19

3.2 Initial Identity Validation 21

3.3 Identification and Authentication for Re-key Requests 25

3.4 Identification and Authentication for Revocation Requests 26

4. Certificate Life-Cycle Operational Requirements 29

4.1 Notification mechanism 29

4.2 Certificate application 29

4.3 Certificate application processing 31

4.4 Certificate issuance 32

4.5 Certificate acceptance 33

4.6 Key pair and certificate usage 34

4.7 Certificate renewal 36

4.8 Certificate re-key 37

4.9 Certificate modification 39

4.10 Certificate revocation and suspension 40

4.11 Certificate status services 50
4.12 End of Subscription 51
4.13 Key escrow and recovery policy and practices 51
5. Facility Management and Operational Controls 51
5.1 Physical Security Controls 51
5.2 Procedural Controls 54
5.3 Personnel Controls 56
5.4 Audit Logging Procedures 59
5.5 Records Archival 65
5.6 Key Changeover 67
5.7 Compromise and Disaster Recovery 68
5.8 LAWtrust AeSign Certification Authority 2048 or LAWtrust AeSign Certificate Authority RA termination 69
6. Technical Security Controls 69
6.1 Key Pair Generation and Installation 69
6.2 Private Key Protection and Crypto-Module Engineering Controls 71
6.3 Other Aspects of Key Pair Management 73
6.4 Activation Data 74
6.5 Computer Security Controls 75
6.6 Life-Cycle Security Controls 76
6.7 Network Security Controls 76
6.8 Time Stamping 77
6.9 Information security 77
6.10 Escalation of information security violations 77
6.11 Secure communication between the RA and the CA 77
6.12 Security Management 77
7. Certificate, CRL, OCSP and System Certificate Profiles 78
7.1 Certificate Profile 78
7.2 CRL Profile 82
7.3 OCSP Profile 83

7.4 System Certificate Profiles 84

8. Compliance Audit and Other Assessments 84

8.1 Frequency of Audit or Assessments 84

8.2 Identity and Qualifications of Assessor 84

8.3 Assessor's Relationship to Assessed Entity 85

8.4 Topics Covered By Assessment 85

8.5 Actions Taken As A Result of Deficiency 85

8.6 Communication of Results 85

9. Other Business and Legal Matters 85

9.1 Fees 85

9.2 Financial Responsibility 87

9.3 Confidentiality of business information 87

9.4 Privacy of Personal Information 89

9.5 Intellectual Property Rights 91

9.6 Representations and Warranties 91

9.7 Disclaimers of Warranties 96

9.8 Limitations of Liability 96

9.9 Indemnities 97

9.10 Term and Termination 97

9.11 Individual Notices and Communications with Participants 97

9.12 Amendments 98

9.13 Dispute Resolution Procedures 99

9.14 Governing Law 99

9.15 Compliance with Applicable Law 100

9.16 Miscellaneous Provisions 100

9.17 Other Provisions 102

10. Appendix A: Definitions 103

11. Sign Off Acceptance 111

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 AeSign Certification Authority 2048 In particular, this CPS establishes the processes and procedures the LAWtrust AeSign Certification Authority 2048 follow to:

- Issue Subscribers' certificates in compliance with the LAWtrust AeSign Certification Authority 2048 and this CPS,
- Manage certificate life cycle for the end entity certificates issued under this LAWtrust AeSign Certification Authority 2048 hierarchy; and
- Operate a directory of issued end user certificates; and
- Operate the CRL directory.

LAWtrust AeSign Certification Authority 2048 is hosted in the LAWtrust data centre which is responsible for managing LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 are labelled "No Stipulation"

1.1 Overview

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

1. LAWtrust AeSign Certification Authority 2048 (LAWtrust AeSign Certification Authority 2048);

The LAWtrust AeSign Certification Authority 2048 CPS describes the certification practices that have been implemented to ensure the LAWtrust AeSign Certification Authority 2048's trustworthiness in issuing public key certificates to Subscribers. It has been drafted to satisfy

the requirements of the LAWtrust Certificate Policy (CP) for issuing LAWtrust Subscriber Certificates.

This LAWtrust AeSign Certificate Authority 2048 CPS is intended to allow participants to the LAWtrust Public Key Infrastructure (PKI) to assess the trustworthiness of the LAWtrust AeSign Certification Authority 2048 and determine suitability of LAWtrust Certificates in meeting their requirements in the communication of electronic information.

1.1.1 Certificate Policy

X.509 certificates issued by LAWtrust AeSign Certification Authority 2048 to subscribers 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 AeSign Certification Authority 2048 as governed by LAWtrust CP and related documents which describe LAWtrust AeSign Certification Authority 2048 requirements and use of Certificates.

1.1.3 Interaction with other PKIs

The LAWtrust AeSign Certification Authority 2048 will not directly interact with other external Certificate Authorities, it will only be chained to the LAWtrust Root CA (2048).

1.1.4 Scope

This CPS applies to subscriber certificates issued by the LAWtrust AeSign Certification Authority 2048

The LAWtrust AeSign Certification Authority 2048 operates under the LAWtrust Public Key Infrastructure (PKI) hierarchy, maintained and operated by LAWtrust for issuance and management of certificates and revocation lists under the hierarchy.

1.2 Document Name and Identification

This document title is “LAWtrust AeSign Certification Authority 2048 Practice Statement (LAWtrust AeSign Certification Authority 2048 CPS)” and is identified by the following object identifier (OID):

The OID for this CPS is : **1.3.6.1.4.1.54383.1.1.1**

You may consider the version of the LAWtrust AeSign Certification Authority 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

The LAWtrust AeSign Certification Authority 2048 is chained into the public hierarchy of the LAWtrust Root Certificate Authority. This CPS includes the practices for the LAWtrust AeSign Certification Authority 2048. This offers certificates with the following hierarchies.

1.3.1.1 Certification Authority

LAWtrust Root Certification Authority 2048

↳ LAWtrust AeSign Certification Authority 2048 (cn=LAWtrust AeSign Certification Authority 2048)

↳ Subscriber

The LAWtrust AeSign Certification Authority 2048 may:

- Accept the certificate signing requests (“CSR”) with the public keys of an Applicant from a LAWtrust AeSign Certificate Authority RA or RA-Agent which has authenticated the identity and verified information to be contained in the LAWtrust AeSign Certification Authority 2048 Certificate applied for by the Applicant;

- Once the CSR is verified the LAWtrust AeSign Certification Authority 2048 will create a LAWtrust AeSign Certification Authority 2048 Certificate containing the signed public key.

A LAWtrust AeSign Certification Authority 2048 Certificate created in response to the CSR will be digitally signed by the LAWtrust AeSign Certification Authority 2048.

1.3.2 Registration Authority and RA-Agents

LAWtrust is a Registration Authority providing Digital Certificate Lifecyle management services to applicants, subscribers and relying parties. LAWtrust may outsource some or all the digital certificate lifecycle responsibilities to separate legal entities. When an outsourced partner is appointed, the entity will be referred to as a RA-Agent.

LAWtrust may appoint RA-Agents in South Africa and in countries which have adopted suitable Electronic Transactions legislation. The suitability of the legislation will be approved by the LAWtrust Policy Authority.

1.3.2.1 Responsibilities of a RA-Agent

LAWtrust may authorise the RA-Agent (as agreed in a Registration Authority Agreement or other Agreements with the RA) to:

- Accept applications for a LAWtrust AeSign Certification Authority 2048 Certificate
- Perform authentication of identities and verification of information submitted by Applicants when applying for a LAWtrust AeSign Certification Authority 2048 Certificate in terms of the LAWtrust Registration Authority Charter (LAWtrust AeSign Certificate Authority RA Charter) approved by the LAWtrust Policy Authority (LAWtrust PA); where such authentication and verification is successful, submit the CSR to the LAWtrust AeSign Certification Authority 2048, in accordance with the provisions of this LAWtrust AeSign Certificate Authority 2048 CPS

- Secure the part of the certificate lifecycle processes for which the RA-Agent assumes responsibility as stated in the LAWtrust AeSign Certificate Authority RA Charter.

1.3.2.2 RA-Agent Identity verification

The identity of a prospective RA-Agent will be verified is the same manner as described in the section covering organisation identity verification clause in 3.2.2.

1.3.3 Subscribers

A Subscriber is a person, entity, or organisation that has been issued a LAWtrust AeSign Certification Authority 2048 Certificate. A subscriber will be issued with a client SSCD, on which the electronic signature creation data (SCD) will be generated. The SCD will be protected by the authentication scheme as specified in the LAWtrust AeSign Certificate Authority RA Charter, ensuring that the subscriber maintains sole control of the SCD. The SCD will include the digital certificate private key. The client SSCD will include the public key certificate.

Subscriber
↳Secure Signature Creation Device (SSCD)
↳Electronic Signature Creation Data (SCD) *{private key}*
↳Public Key Certificate

From a subscriber point of view electronic signature creation data (SCD) and private key can be used interchangeably.

1.3.3.1 Applicants

An Applicant is a person, entity, or organisation that has applied for but has not yet been issued a LAWtrust AeSign Certification Authority 2048 Certificate.

1.3.4 Relying parties

A Relying Party is a person, entity, or organisation that relies on or uses a LAWtrust AeSign Certification Authority 2048 Certificate and/or any other information provided in the LAWtrust repository to verify the digital signature Subscriber.

1.3.5 Other participants

1.3.5.1 LAWtrust Security Committee

LAWtrust Security Committee is responsible for the approval of PKI Policies and overseeing the security operations of the LAWtrust AeSign Certification Authority 2048

1.3.5.2 LAWTRUST Policy Authority (LAWTRUST PA)

The LAWTRUST Policy Authority (LAWTRUST PA) is an assigned role responsible for the development, maintenance of the LAWTRUST PKI Policies, amongst other duties.

1.4 Certificate Usage

The LAWtrust AeSign Certification Authority 2048 is capable of manufacturing X.509 V3 digital certificates for the purposes outlined below

1.4.1 Appropriate Certificate Uses

LAWtrust AeSign Certification Authority 2048 Certificates may be used to digitally sign electronic documents and transactions. In particular

- Digital signatures
- Non-repudiation

1.4.2 Prohibited Certificate Uses

LAWtrust AeSign Certification Authority 2048 Certificates are not designed or intended for use in or in conjunction with hazardous activities or uses, requiring failsafe performance and the use of the certificates in this regard is strictly prohibited.

Any use falling outside the LAWtrust AeSign Certification Authority 2048 Certificate uses described in this LAWtrust AeSign Certificate Authority 2048 CPS shall be deemed a prohibited 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 AeSign Certificate Authority 2048 CPS shall be directed at:

Email: governance@lawtrust.co.za

Telephone: +27 12 676 9240

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 AeSign Certification Authority 2048 conform to the requirements of the LAWtrust CP in accordance with policies and procedures specified by LAWtrust.

1.5.4 CPS approval procedures

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

The LAWtrust AeSign Certificate Authority 2048 CPS is developed by the LAWtrust PA and the LAWtrust OA and approved by the LAWtrust Security Committee (SC) and signed off by the PA. Approved documents shall be published in the LAWtrust repository with a notification of such an update.

1.5.4.1 Process for CPS change requests

The LAWtrust AeSign Certification Authority 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 **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 AeSign Certification Authority 2048 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 AeSign Certification Authority 2048 CPS,
- Information and agreements relating to the subscription for and reliance on LAWtrust Subordinate CA Certificates;

- The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 CPS.

b. Certificate Status Repository

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

- CRL1 (web interface access):

  The LAWtrust AeSign Certification Authority 2048 Certificate Revocation List (CRL's) is accessible through the web-interface:

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

  and is periodically updated in terms of the **LAWtrust AeSign Certification Authority 2048** CPS.

- Online Certificate Status Protocol

  OCSP Responses are available 24 hours a day, 7 days a week as described in section 4.10.12, with time allocated for general maintenance of the OCSP Responder.

2.1.1 Repository Obligations

The repository capabilities that LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 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 AeSign Certification Authority 2048 issued certificates and CRLs and to prevent modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of the LAWtrust AeSign Certificate Authority 2048 CPS

This LAWtrust AeSign Certificate Authority 2048 CPS, published in the LAWtrust repository, shall be available by web-interface [*https://www.lawtrust.co.za/repository*] at all times subject to any interruption of the LAWtrust website services.

Changes or modifications to this LAWtrust AeSign Certificate Authority 2048 CPS shall be published in accordance with directions given by the LAWtrust PA.

2.2.2 Publication of Certificates and Certificate Status

The LAWtrust AeSign Certification Authority 2048 maintain repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 repositories shall contain the following PKI related elements:

- LAWtrust AeSign Certification Authority 2048 certificate 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.

2.2.3 Publication and notification policies

The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 reserves the right to publish newer versions of the documentation without prior notice.

Additionally, the LAWtrust AeSign Certification Authority 2048 will publish an approved, current and digitally signed version of its CP and CPS.

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

- All accessible certificates issued by LAWtrust AeSign Certification Authority 2048: and
- The certificate revocation list (CRL) for the LAWtrust AeSign Certification Authority 2048.

2.2.4 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 CPS shall be published in the manner described in section 2.2

The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 provide certificates.
- Annual Review of the LAWtrust AeSign Certification Authority 2048 CPS.

Changes shall be documented in revised versions of the LAWtrust AeSign Certification Authority 2048 CPS and become effective on the dates indicated in the revised CPS.

2.4 Access Controls on Repositories

The LAWtrust AeSign Certification Authority 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 certificate a RA-Agent shall authenticate the identity and/or attributes of an Applicant to be published in a LAWtrust AeSign Certification Authority 2048 Certificate. This section of the LAWtrust AeSign Certificate Authority 2048 CPS establishes the criteria for an

acceptable application for a LAWtrust AeSign Certification Authority 2048 Certificate and for the authentication of persons requesting the revocation of a LAWtrust AeSign Certification Authority 2048 Certificate.

3.1 Naming

3.1.1 Types of Names

A LAWtrust AeSign Certification Authority 2048 Certificate shall include a common name component as required in the X.501 Standard. The common name shall be the name as stated on the applicant's identity document.

3.1.2 Need for Names to be Meaningful

3.1.2.1 Naming Subscribers for Personal Certificates:

The value of the common name attribute used in naming Subscribers is as a minimum, the combination of a first name and surname of the Subscriber and one other unique identifier for example email address registered on the application or other identifier.

3.1.2.2 Naming Subscribers for Entity Certificates:

The value of the common name attribute used in naming Subscribers for Entity certificates is the name, in the case of any Entity that requires registration as a minimum, the Entity Name or shortened name and the Entity's registration number.

The LAWtrust RA is the only entity which is permitted to issue entity certificates. The RA-Agents are not permitted to issue entity certificates.

3.1.3 Anonymity or Pseudonymity of Subscribers

LAWtrust shall only provide anonymous certificates or certificates to individuals under a pseudonym for dedicated Certificate Authority roles.

In cases where the LAWtrust AeSign Certification Authority 2048 or RA has to issue certificates for the purposes of testing or demonstration the certificate will be referred to as a "demo certificate". These demo certificates may be used exclusively for internal testing, demonstration and presentation purposes and not for any secure or confidential communications. Demo certificates may be used by authorized users only. The test certificate should have the text "First name Surname Demo Certificate" or any identifiable text like "Test" in the common name.

3.1.4 Rules for Interpreting Various Name Forms

In the provision of personal certificates, the names and other attributes in the certificate distinguished name of persons will provide a unique name.

LAWtrust AeSign Certification Authority 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

3.1.5.1 Personal Identities

The combination of the common name and other company specific attributes contained in the Distinguished Name (DN), together with the serial number attributed to the certificate provides

a unique electronic identity for the person associated with the certificate. LAWtrust shall not re-use a serial number in respect of a LAWtrust AeSign Certification Authority 2048 Certificate.

3.1.5.2 Legal Identities

The Entity Distinguished name will provide uniqueness by including the duly authorised legal entity details in the common name.

3.1.6 Name claim dispute resolution

The common names in LAWtrust AeSign Certification Authority 2048 Certificates are issued on a “first come, first served” basis. By accepting a common name for incorporation into a LAWtrust AeSign Certification Authority 2048 Certificate, an RA operating under a LAWtrust AeSign Certification Authority 2048 does not determine whether the use of such information infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property right or any other rights of any person, entity, or organization. The LAWtrust AeSign Certification Authority 2048 and any RA’s operating under the LAWtrust AeSign Certification Authority 2048 neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in a LAWtrust AeSign Certification Authority 2048 Certificate.

3.1.7 Recognition, Authentication and Role of Trademarks

Certain terms such as LAWtrust and AeSign are trademarks of LAWtrust. LAWtrust may make use of other trademarks with permission of the relevant owner of the trademark. Any trademark dispute will be dealt with in terms of Section 9.12 of this CPS.

3.2 Initial Identity Validation

The RA-Agent will establish reasonable proof of identity of the person depending on the nature of the subscriber (natural person and or other) and the use of the certificate. The LAWtrust AeSign Certificate Authority RA Charter will stipulate the information required for

authentication of the identity and the method of authentication and verification of the information as described in the sections below and as approved by the LAWtrust PA.

3.2.1 Method to prove possession of private key

The method of proving possession of a private key will be authorised by the LAWtrust PA and stated in the LAWtrust AeSign Certificate Authority RA Charter.

3.2.1.1 Possession at registration

At registration, possession of the private key corresponding to a supplied public key is achieved when control of an approved SSCD is handed over to the applicant.

Handing control of a client SSCD over to applicant subscriber is achieved by the process of the applicant creating the SSCD password overseen by the enrolment officer or governed by a process approved by the LAWtrust PA.

No further proof of possession is required at the time of registration.

If the process of handing over control as described in this section cannot be achieved, then the process described in section 3.2.1.2 below should be adhered to.

3.2.1.2 Possession other than registration

In cases were handing over control as described in this section 3.2.1.1 cannot be achieved, or during processes where the CA or RA require the cryptographic proof of possession of the private key then the process below should be adhered to;

1. The Subscriber should digitally sign a data message with their private key
2. The signed data message together with the subscriber public key and the original unencrypted message should be made available to the RA or CA.
3. The RA or CA will then
    a. Check that the certificate is valid (not revoked, not suspended, not expired).

b. verify the signature by decrypting the encrypted data message, and compare it to the original data message.

In all instances in which the LAWtrust AeSign Certificate Authority RA Charter does not specifically provide for proof of possession of the private key, the onus of proving possession of the private key will fall on the Subscriber.

3.2.2 Authentication of organisation identity

In the case where the organisation is registered in South Africa, sections 3.2.2.1 and 3.2.2.2 will apply.

In the case where the applicants are citizens of a foreign country and the organisation is registered in that country, the organization will be validated against the foreign country's national database or company registry, using the principles as documented in sections 3.2.2.1 and 3.2.2.2 where applicable. Evidence to confirm such registration may be requested by LAWtrust and must be provided by the organisation.

3.2.2.1 Authentication of a company, close corporation, or other legal Entity

Where the subscriber is a company, close corporation, or other legal Entity

1. a valid search done through Companies and Intellectual Property Commission (CIPC) or other accredited CIPC search provider or a Disclosure Certificate issued by CIPC,
2. the relevant constitutive documents,
3. a letter on a company letterhead, signed by a duly authorised person indicating the authority for the applicant to apply for the certificate on behalf of the company; and
4. the identity documents applicable for natural persons for the applicant.

3.2.2.2 Authentication of partnerships

Where the subscriber is a partnership,

1. the constitutive documents of the partnership, if applicable and

2. the identity documents applicable for natural persons.

3.2.3 Authentication of individual identity

3.2.3.1 Authentication of natural persons

Where the subscriber is a natural person, the following documents must be used

1. Identity document for initial registration. (See Definition of Identity document in clause 1.6).

2. Accredited certificate for Certificate renewal

3.2.3.2 Authentication of a personal identity eMail address

In cases where the LAWtrust AeSign Certification Authority 2048 Certificate will be used for digitally signing the RA-Agent will establish reasonable proof that the person or legal Entity submitting the certificate request controls the eMail account associated with the eMail address referenced in the LAWtrust AeSign Certification Authority 2048 Certificate.

3.2.4 Non-verified Subscriber information

Certain information gathered for certification may not be verified by a RA-Agent. All the information published in a LAWtrust AeSign Certification Authority 2048 Certificate shall be verified by RA-Agent as stipulated by the LAWtrust PA.

3.2.5 Validation of authority

The LAWtrust AeSign Certification Authority 2048 is the authority to which any RA's under the LAWtrust AeSign Certification Authority 2048 have been created. As such all rights, entitlements, or permissions of Subscribers within a RA-Agent are stipulated in the LAWtrust AeSign Certificate Authority RA Charter.

3.2.6 Criteria for interoperation

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

A RA-Agent shall establish proof of identity of the person or entity and authenticate the identity of the Applicant and verify the accuracy of information to be published in a LAWtrust AeSign Certification Authority 2048 Certificate subject to a routine re-key in the manner determined in the LAWtrust AeSign Certificate Authority RA Charter. The stringency of authentication of identity and verification of information shall be commensurate with the minimum stipulations of the LAWtrust PA for the certification required.

3.3.2 Identification and Authentication for Re-key After Revocation

The LAWtrust AeSign Certification Authority 2048 shall not renew or re-issue LAWtrust AeSign Certification Authority 2048 Certificates that have been permanently revoked.

A Subscriber who wishes to use a LAWtrust AeSign Certification Authority 2048 Certificate after revocation must apply for a new LAWtrust AeSign Certification Authority 2048 Certificate to replace LAWtrust AeSign Certification Authority 2048 Certificate that has been revoked.

A Subscriber shall be required to complete a new application process as described in section 3.2 including generation of a new key-pair and submission of all information required for an initial application for a LAWtrust AeSign Certification Authority 2048 Certificate as stipulated in the LAWtrust AeSign Certificate Authority RA Charter.

On revocation of a LAWtrust AeSign Certification Authority 2048 Certificate the Subscriber shall immediately cease using such a LAWtrust AeSign Certification Authority 2048 Certificate

and remove the LAWtrust AeSign Certification Authority 2048 Certificate from any devices and/or software in which it has been installed.

3.4 Identification and Authentication for Revocation Requests

A LAWtrust AeSign Certificate Authority RA shall provide for the manner in which authentication of the identity of any person requesting revocation of a certificate is established. These provisions will be contained in the LAWtrust AeSign Certificate Authority RA Charter which shall be approved by the LAWtrust PA.

3.4.1 Access and permissions to revoke

The only personnel who are authorised to perform revocations must satisfy the following criteria;

1. The appointed RA-Agent must nominate RA-Agent personnel to be the certificate administrators.

2. The nominated RA-Agent personnel must fill in an application form, sign the application form

3. The application form must be collected in person by a LAWtrust appointed resource, who will perform a face-to-face identity verification and view the identity document presented.

On application form receipt and approval, the LAWtrust administrator will create the administrator on the LAWtrust AeSign Certification Authority 2048. The permissions will be restricted to the specific RA-Agent concerned.

In the case of an API being used, the request is authenticated via the unique TSO agent

3.4.2 Revocation Request format

Revocation requests may be sent to the RA-Agent email address as specified in the LAWtrust AeSign Certificate Authority RA Charter.

The format of the request should include the following:

1. Requester name, designation and organisation
2. Reason for and severity of the revocation request
    a. Severity 1: suspected key and or password compromise,
    b. Severity 2: lost, stolen or corrupted key store,
    c. Severity 3: Business related reason (end of business relationship of change in permissions) or other valid reasons.
3. Provide details of the events leading up to the point of defining a reason
4. Date and time of any events, relating to the reason for the revocation request.

The request should be digitally signed by the requester

3.4.3 Procedures to verify a revocation request

A revocation request will be verified in the manner stipulated in section 4.10.3.

If the request originates from the subscriber or other appropriately authorised party the certificate to be revoked, the administrator will

1. Verify that the request originates from an administrator of an appointed RA.
2. Verify the digital signature of the email if signed.

3. Make every effort to verify the email address of the subscriber, by records or by challenge response

4. Make every effort to contact the organisation of the requester to inform them.

3.4.4 Procedures for processing revocation requests

Once the administrator has received the request, the administrator will verify the request and respond to the request within the timeline specified for each severity.

In the procedure below all time is measured from when the request is received by the RA administrator.

3.4.4.1 Severity 1: suspected key and or password compromise,

1. Revocation performed by the Administrator within 4 hours of the revocation request being acknowledged,

2. CRL update occurs within a few minutes of revocation being performed.

3. OCSP update cycle, 30 minutes

3.4.4.2 Severity 2: lost, stolen or corrupted SSCD

1. Revocation performed within 8 hours of the revocation request being acknowledged.,

2. CRL update occurs within a few minutes of revocation being performed.

3. OCSP update cycle, 30 minutes

3.4.4.3 Severity 3: Business related

1. Revocation performed within 24 hours of the revocation request being acknowledged,

2. CRL update occurs within a few minutes of revocation being performed.

3. OCSP update cycle, 30 minutes

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

LAWtrust appoints the RA-Agent's to perform the certificate lifecycle operations and management according to the processes specified in the LAWtrust AeSign Certificate Authority RA Charter. The process of a RA-Agent authorisation and appointment is set out in clause 1.3.2 of this CPS as stipulated in the SAAA Accreditation Regulations on the delegation of certificate lifecycle functions to agents.

All RA-Agent responsibilities relating to the processes and security are included in the LAWtrust AeSign Certificate Authority RA Charter. Any variations (peculiar to a LAWtrust AeSign Certificate Authority RA) from the LAWtrust AeSign Certificate Authority RA Charter, will be documented in a Process Flow Annexure.

4.1 Notification mechanism

Certificate lifecycle notification between the LAWtrust AeSign Certificate Authority RA and the applicant\Subscriber or between the CA and the applicant\subscriber will provide for an audit trail evidencing that the notification occurred.

4.2 Certificate application

4.2.1 Who can submit a certificate application?

An Applicant or an Applicant's manager performing duties as stipulated in the LAWtrust AeSign Certificate Authority RA Charter may submit a certificate application to the approved LAWtrust AeSign Certificate Authority RA. RA-Agents are not permitted to issue entity certificates.

The LAWtrust AeSign Certification Authority 2048 shall, under this LAWtrust AeSign Certificate Authority 2048 CPS, issue:

1. LAWtrust AeSign Certification Authority 2048 Certificates in respect of natural persons.

2. LAWtrust AeSign Certification Authority 2048 Certificates in respect of recognised entities.

4.2.2 Enrolment process and responsibilities

4.2.2.1 Applicants

1. Complete and submit to a LAWtrust AeSign Certificate Authority RA an application for a LAWtrust AeSign Certification Authority 2048 Certificate providing all information requested, without any errors, misrepresentations or omissions;

2. In making the application, agree to be bound by the terms of this LAWtrust AeSign Certificate Authority 2048 CPS and the applicable Subscriber Agreement;

3. Make payment to the LAWtrust AeSign Certification Authority 2048 and/or LAWtrust AeSign Certificate Authority RA of all fees and charges in respect of the application for the issue of the LAWtrust AeSign Certification Authority 2048 Certificate.

4.2.2.2 Registration Authority Agent LAWtrust AeSign Certificate Authority RA

On receipt of a properly completed application, a RA-Agent shall process the application and verify the information provided in terms of section 3.2.

If the application or information provided to the RA-Agent is deficient, the RA-Agent shall:

1. Use reasonable efforts to notify the applicant of the deficiency and of the refusal of the application.

If the verification of the information submitted to the LAWtrust AeSign Certificate Authority RA is successful, then;

1. The LAWtrust AeSign RA shall submit a CSR to the LAWtrust AeSign CA;

2. Notify the Applicant, at the eMail address provided in the application or in person, that the CSR has been submitted to the LAWtrust AeSign CA and of the instructions to follow for the Applicant to retrieve the LAWtrust AeSign CA Certificate when issued.

3. Assist the applicant with the retrieval and installation of the LAWtrust AeSign Certification Authority 2048 Certificate onto the SSCD which has been issued to them.

After the issue of the LAWtrust AeSign Certification Authority 2048 Certificate neither the LAWtrust AeSign Certification Authority 2048 nor any LAWtrust AeSign Certificate Authority RA's will have any obligation to perform any ongoing monitoring, investigation or verification of the information provided in the certificate application.

4.2.3 Notifications to the Subscriber

The RA shall make commercially reasonable efforts to notify the applicant and or subscriber of certain digital certificate lifecycle events. Notification's to the applicant or subscriber will be performed either in person or via Email, using the eMail address documented in the application form, unless a different mechanism is specified in the LAWtrust AeSign Certification Authority 2048 Charter.

4.3 Certificate application processing

4.3.1 Performing identification and authentication functions

The LAWtrust AeSign Certification Authority 2048 shall process an application for the issue of a LAWtrust AeSign Certification Authority 2048 Certificate only after a LAWtrust AeSign Certificate Authority RA has performed the authentication and verification checks provided for in the LAWtrust AeSign Certificate Authority RA Charter.

4.3.1.1 Verification checks to be performed

The following verification checks will be performed to confirm the identity of the applicant\subscriber;

1. Perform face-to-face identification of the subscriber or authorised key holder. This process entails comparing the applicant\subscriber facial features with the photo in an approved identity document.

2. The face-to-face identification process will be performed in such a way that the process is demonstrable and auditable.

3. Verify any further information submitted by the subscriber which will be included in the certificate contents.

Once the authentication and verification process has been completed the LAWtrust AeSign Certificate Authority RA shall retain all relevant information and confirmation of the authentication or verification, in conformance with the requirements of the LAWtrust PA, as set out in section 5.5 of this CPS.

4.3.2 Approval or rejection of certificate applications

Approval of a certificate application will result in the process continuing. Application rejection may result in notification by the LAWtrust AeSign Certificate Authority RA to the applicant of the reason for the rejection, as set out in section 4.2.2.

4.3.3 Time to process certificate applications

Any application for a certificate should be processed within the time stipulated in the LAWtrust AeSign Certificate Authority RA Charter. The LAWtrust AeSign Certification Authority 2048 will process the request immediately on receiving such a request.

4.3.4 Time to publish certificates in the certificate directory

The LAWtrust AeSign Certification Authority 2048 will publish digital certificates into the certificate directory, immediately on processing such a request.

4.4 Certificate issuance

4.4.1 CA actions during certificate issuance

The LAWtrust AeSign Certification Authority 2048 can only accept certificate issuance requests from authorised LAWtrust AeSign Certificate Authority RA instances. These RA

components are authenticated using a secure certificate management protocol between the LAWtrust AeSign Certificate Authority RA component and the LAWtrust AeSign Certification Authority 2048. After satisfying itself that the authentication have been executed, the LAWtrust AeSign Certification Authority 2048 may generate and digitally sign the LAWtrust AeSign Certification Authority 2048 Certificate applied for in accordance with the certificate profile described in section 7.1 of this LAWtrust AeSign Certificate Authority 2048 CPS.

4.4.1.1 Subscriber private key generation and storage

The subscriber's private key is generated by the CA on a secure system on behalf of the subscriber. The private key can be stored in the following approved key stores

1. On a client SSCD

4.4.2 Notification to Subscriber by the RA of issuance of certificate

The certificate is only issued in the presence of the subscriber, so no notification will be sent.

4.5 Certificate acceptance

4.5.1 Conduct constituting certificate acceptance

After issuance of the LAWtrust AeSign Certification Authority 2048 Certificate, the Subscriber shall check that the content of the LAWtrust AeSign Certification Authority 2048 Certificate is correct.

Unless notified to the contrary by the Subscriber of any inaccuracies in the LAWtrust AeSign Certification Authority 2048 Certificate, the LAWtrust AeSign Certification Authority 2048 Certificate shall be deemed to have been accepted by the Subscriber and the information contained in the LAWtrust AeSign Certification Authority 2048 Certificate deemed to be accurate.

By using the LAWtrust AeSign Certification Authority 2048 Certificate in any manner contemplated in this LAWtrust AeSign Certificate Authority 2048 CPS, the Subscriber accepts

the accuracy of the information contained in the LAWtrust AeSign Certification Authority 2048 Certificate.

If the LAWtrust AeSign Certificate Authority RA is notified of any inaccuracies in the LAWtrust AeSign Certification Authority 2048 Certificate by the Subscriber the LAWtrust AeSign Certification Authority 2048 Certificate shall be revoked in terms of the provisions of section 3.4 of this LAWtrust AeSign Certificate Authority 2048 CPS.

4.5.2 Publication of the certificate by the CA

Post issuance the certificate is published in the LAWtrust AeSign Certification Authority 2048 database.

4.5.3 Notification of certificate issuance to other Entities

There are no further communications to other Entities.

4.6 Key pair and certificate usage

4.6.1 Subscriber private key and certificate usage

The Subscriber shall only use the private key associated with the 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 AeSign Certification Authority 2048 Certificate.

The Subscriber shall use his/her private key and the LAWtrust AeSign Certification Authority 2048 Certificate in strict compliance with the Subscriber Agreement entered between the Subscriber and LAWtrust and this LAWtrust AeSign Certificate Authority 2048 CPS.

4.6.1.1 Financial limitations on certificate usage

The value of transactions, financial and other, will be defined by the RA's in their commercial contracts with their business partners or employees using the certificates. Financial liability for

certificate usage will be stipulated in the commercial agreements between LAWtrust and all RA's.

4.6.2 Relying Party public key and certificate usage

Relying Parties shall comply strictly with the provisions of the LAWtrust Relying Party Agreement and shall be responsible for checking the status of any LAWtrust AeSign Certification Authority 2048 Certificate before relying on the certificate.

The relying Party Agreement can be found at the following URL;

https://www.lawtrust.co.za/repository

4.6.3 Subscriber private key generation and storage

The subscriber's private key must be generated under the sole control of the subscriber. The private key will be stored on a client SSCD

4.6.4 Life cycle management of the Client SSCD.

The client SSCD lifecycle can be described as follows

1. SSCDs are ordered from the supplier

2. SSCDs are initialised with the LAWtrust configuration during the enrolment process

3. SSCDs are issued to subscribers, at the same time that the digital certificate requirement for face-to-face identity verification is performed.

4. SSCDs and the digital certificate which resides on the SSCD are used by the subscriber

5. If an SSCD is lost or stolen or compromised, the certificate is revoked and new SSCD and certificate is issued.

6. If subscribers have a change in job status where the new job status excludes the digital signatures and where a validated request is sent by an approved RA, the certificate is revoked, the SSCD is recycled (wiped clean\re-initialised) and reissued to another subscriber.

4.7 Certificate renewal

Certificate renewal is when the key pair of the certificate stays the same, but the validity dates are changed. LAWtrust AeSign Certification Authority 2048 Certificates does not support renewal. Certificates that expire will be re-keyed instead of renewed.

4.7.1 Circumstance for certificate renewal

No Stipulation

4.7.2 Who may request renewal

No Stipulation

4.7.3 Processing certificate renewal requests

No Stipulation

4.7.4 Notification of new certificate issuance to subscriber

No Stipulation

4.7.5 Conduct constituting acceptance of a renewal certificate

No Stipulation

4.7.6 Publication of the renewal certificate by the CA

No Stipulation

4.7.7 Notification of certificate issuance by the CA to other entities

No Stipulation

4.8 Certificate re-key

A Re-key of a LAWtrust AeSign Certification Authority 2048 certificate means creating a new public key and issuing a new certificate with the new public key and serial number. The validity dates, key identifiers, CRL and OCSP distribution point and signing key of the new certificate may differ from the prior certificate.

The LAWtrust AeSign Certification Authority 2048 shall re-key a certificate provided that the RA-Agent conducts and confirms that it has conducted the necessary authentication and verification checks for the purposes of the certificate re-key in accordance with the LAWtrust AeSign Certificate Authority RA Charter approved by the LAWtrust PA.

4.8.1 Circumstance for certificate re-key

The LAWtrust AeSign Certification Authority 2048 shall re-key a certificate under the following conditions;

1. a subscriber requests a certificate and the subscriber certificate has in the past been revoked or has expired or is about to expire.
2. a subscriber suspects that access to the private key is compromised.
3. A subscriber has requested that information in the certificate is amended.

In the case of a valid certificate it will be re-keyed automatically, in the other cases described above the subscriber is required to undergo the full registration process in accordance with the LAWtrust AeSign Certificate Authority RA Charter approved by the LAWtrust PA.

4.8.2 Who may request certification of a new public key

LAWtrust may perform a certificate rekey at its own discretion or at request of an RA or at request by a subscriber.

4.8.3 Processing certificate re-keying requests

In the case that any certificate detail such as subscriber private Key, identity and domain information remains unchanged, a new certificate will be issued.

4.8.4 Notification of new certificate issuance to subscriber

If a Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate requires re-key, the RA-Agent that requested renewal of the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate shall make a commercially reasonable effort to notify the Subscriber via a mechanism as described in section 4.1.

4.8.5 Conduct constituting acceptance of a re-keyed certificate

Unless notified to the contrary by the Subscriber of any inaccuracies in the LAWtrust AeSign Certification Authority 2048 Certificate, the LAWtrust AeSign Certification Authority 2048 Certificate shall be deemed to have been accepted by the Subscriber and the information contained in the LAWtrust AeSign Certification Authority 2048 Certificate deemed to be accurate.

4.8.6 Publication of the re-keyed certificate by the CA

Post re-key the rekeyed certificate is published in the LAWtrust AeSign Certification Authority 2048 database.

4.8.7 Notification of certificate issuance by the CA to other entities

There are no further communications to other entities.

4.8.8 CA certificate re-key

The LAWtrust AeSign Certification Authority 2048 Certificates, signed by the LAWtrust Root Certification Authority 2048, contain a Certificate expiration date. When the LAWtrust AeSign Certification Authority 2048 reaches this expiration date, LAWtrust will re-key the CA, and

process the resulting Certificate Signing Request via the LAWtrust Root Certification Authority. LAWtrust shall make a commercially reasonable effort to notify all Registration Authorities of the pending expiration of the LAWtrust AeSign Certification Authority 2048 Certificate by sending an eMail to the technical contact listed in the LAWtrust Registration Authority contact list. A notification will also be published in the LAWtrust Repository. Upon expiration of the LAWtrust AeSign Certification Authority 2048 Certificate, all Registration Authorities and their Subscribers shall immediately cease using the Certificate and shall remove the LAWtrust AeSign Certification Authority 2048 Certificate from any devices and/or software in which it has been installed.

4.9 Certificate modification

The LAWtrust AeSign Certification Authority 2048 shall not modify certificates.

4.9.1 Circumstance for certificate modification

No Stipulation.

4.9.2 Who may request certificate modification

No Stipulation.

4.9.3 Processing certificate modification requests

No Stipulation.

4.9.4 Notification of new certificate issuance to subscriber

No Stipulation.

4.9.5 Conduct constituting acceptance of modified certificate

No Stipulation.

4.9.6 Publication of the modified certificate by the CA

No Stipulation.

4.9.7 Notification of certificate issuance by the CA to other entities

There are no further communications to other entities.

4.10 Certificate revocation and suspension

A certificate is suspended if an event which may result in a revocation is suspected and not confirmed. A certificate is revoked when there is reasonable evidence to believe that certain events took place which warrant the revocation of the certificate as more specifically defined in 4.10.1.

The LAWtrust AeSign Certification Authority 2048 shall revoke a LAWtrust AeSign Certification Authority 2048 Certificate after receiving a valid revocation request from any RA-Agent.

A RA-Agent. shall be entitled to request revocation of a certificate and the LAWtrust AeSign Certification Authority 2048 shall be entitled to revoke Subscriber's LAWtrust AeSign Certification Authority 2048 Certificates, if the RA-Agent. or LAWtrust AeSign Certification Authority 2048 acquires knowledge of or has a reasonable basis for believing that any of the events as described in section 4.10.1 has occurred.

4.10.1 Circumstances for revocation

A Subscriber shall request revocation of their LAWtrust AeSign Certification Authority 2048 Certificate if the Subscriber has a suspicion or knowledge of a compromise of the Subscriber's private key or that the information contained in the Certificate has become inaccurate, incomplete, or misleading as a result of change in circumstances relating to the Subscriber.

A request for revocation by a Subscriber shall be submitted to a RA-Agent and processed according to the processes defined in section 4.10.3 and the LAWtrust AeSign Certificate Authority RA Charter (with the Subscriber's application for a new LAWtrust AeSign Certification Authority 2048 Certificate if applicable).

LAWtrust AeSign Certification Authority 2048 subscriber Certificates may be revoked under authority from the LAWtrust Operations Authority under the following circumstances:

1. Abuse of the digital certificate by the subscriber.
2. Subscriber's request.
3. Any change in the information contained in the LAWtrust AeSign Certification Authority 2048 Certificate issued to a Subscriber;
4. Subscriber suspected of fraudulent activity.
5. The compromise of the LAWtrust AeSign Certification Authority 2048 private key, or if applicable, the compromise of a superior Certification Authority's private key;
6. Breach by the Subscriber of any of the terms of this LAWtrust AeSign Certificate Authority 2048 CPS or the Subscriber Agreement entered into with the Subscriber;
7. Non-payment of fees in respect of any services provided by LAWtrust or RA-Agent.
8. Issue or use of the certificate not in accordance with the LAWtrust AeSign Certificate Authority 2048 CPS.
9. If a subscriber dies and after receiving a certified copy of the subscriber's death certificate.
10. On receipt of documentary proof that a subscriber that is a legal person has been wound up, or deregistered or has ceased to exit.
11. The LAWtrust AeSign Certification Authority 2048 or LAWtrust Root CA 2048 expires.

12. A determination by the LAWtrust AeSign Certification Authority 2048 or a RA-Agent. that the certificate was not issued in accordance with this LAWtrust AeSign Certificate Authority 2048 CPS or the provisions of the Subscriber's Agreement entered into with the Subscriber; or

13. Any other reason that the LAWtrust AeSign Certification Authority 2048 reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust AeSign Certification Authority 2048 Certificate.

Revocation of a LAWtrust AeSign Certification Authority 2048 subscriber Certificate shall not affect any of the Subscriber's contractual obligations under this LAWtrust AeSign Certificate Authority 2048 CPS or the Subscriber's Agreement entered into by the Subscriber or any Relying Party Agreements.

4.10.2 Who can request revocation

A Subscriber may request revocation of his/her LAWtrust AeSign Certification Authority 2048 Certificate at any time and for any reason. Subscriber requests for revocation will be facilitated by the RA-Agent.

The LAWtrust AeSign Certification Authority 2048 or RA-Agent may request revocation of a LAWtrust AeSign Certification Authority 2048 subscriber Certificate if it reasonably believes that the subscriber no longer requires the certificate or the LAWtrust AeSign Certification Authority 2048 Certificate or private key associated with the LAWtrust AeSign Certification Authority 2048 Certificate has been compromised.

Before revoking a certificate at the request of a Subscriber the LAWtrust AeSign Certification Authority 2048 shall use commercially reasonable efforts to validate the identity of the Subscriber or the person representing the Subscriber and shall not be required to revoke the LAWtrust AeSign Certification Authority 2048 subscriber Certificate until it is satisfied as to the identity of the Subscriber. The Subscriber shall comply with any reasonable requests of the LAWtrust AeSign Certification Authority 2048 relating to validating the identity of the Subscriber making a revocation request.

4.10.3 Procedure for revocation request

A RA-Agent shall authenticate a request by a Subscriber for revocation of his/her LAWtrust AeSign Certification Authority 2048 Certificate by requiring:

4.10.3.1 Initiate revocation requests

A Subscriber shall initiate a revocation request following the process as documented in section 3.4.2

4.10.3.2 Verification and Authentication of revocation requests

Revocation requests to RA-Agent by subscribers will be authenticated by verifying that the requester was issued with a digital certificate by the LAWtrust AeSign Certification Authority 2048 via the RA-Agent. The subscriber verification check will include checking that the subscriber email address in the digital certificate is indeed the email address used to initiate the revocation request.

Revocation requests to the RA-Agent via a RA-Agent will be authenticated by checking whether the RA-Agent has a contractual agreement with the LAWtrust AeSign Certification Authority 2048 and that the agent is authorised to facilitate the issuance of a LAWtrust AeSign Certification Authority 2048 digital certificate to the subscriber.

4.10.3.3 Perform the revocation

Once the verification and authorisation of the revocation request has been performed the administrator will change the status of the certificate to revoked and include the reason for the revocation as provided in section 3.4.2

4.10.3.4 Notification of revocation

Notification and certificate status publication process will be followed.

1. If a Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate is revoked for any reason, the RA-Agent that requested revocation of the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate shall make a commercially reasonable

effort to notify the Subscriber by sending an email to the email address provided in the certificate application.

2. The LAWtrust AeSign Certification Authority 2048 certificate revocation lists will be updated as per the schedule specified in section 3.4.4. The serial number of the revoked LAWtrust AeSign Certification Authority 2048 subscriber Certificate will be posted to the CRL located at the locations specified in section 2.1.

4.10.4 Bulk Revocation request

A RA-Agent may request a LAWtrust AeSign Certification Authority 2048 to revoke LAWtrust AeSign Certification Authority 2048 subscriber Certificates in bulk in accordance with the provision of the LAWtrust AeSign Certificate Authority RA Charter as approved by the LAWtrust PA.

4.10.4.1 Identifying the certificates to be included in a bulk revocation

The certificates to be included in a bulk suspension are identified by any circumstances as described in section 4.10.1

4.10.4.2 Procedure for bulk revocation request

A RA-Agent may request a LAWtrust AeSign Certification Authority 2048 to revoke LAWtrust AeSign Certification Authority 2048 subscriber Certificates in bulk in accordance with the provision of the LAWtrust AeSign Certificate Authority RA Charter as approved by the LAWtrust PA.

The LAWtrust AeSign Certification Authority 2048 certificate administrator on receiving the bulk revocation request with the details of the Subscribers' accounts and LAWtrust AeSign Certification Authority 2048 subscriber Certificate serial numbers, shall prepare a list of certificate accounts to be send to the LAWtrust AeSign Certification Authority 2048 for bulk revocation.

The LAWtrust AeSign Certification Authority 2048 on receiving the bulk revocation request submitted by the LAWtrust certificate administrator, shall determine the timeframes for the

bulk revocation using information provided in section 3.4.4, process the bulk revocation request and post the serial numbers of the revoked Certificates to the CRL in the LAWtrust repositories as specified in section 2.1

Notification and publication of the certificate revocation lists will be updated as per the schedule specified in section 3.4.4.

4.10.5 Revocation request grace period

In the case of a private key compromise or suspected private key compromise, the Subscriber shall initiate a request to revoke the associated Certificate immediately upon detection of the compromise or suspected compromise.

Revocation requests for other required reasons shall be made as soon as reasonably practicable as per the process documented in section 3.4.4.

4.10.6 Time to process the revocation request

The LAWtrust AeSign Certification Authority 2048 shall issue CRL's at least once every 24 hours. In certain circumstances CRL's may also be issued between these intervals, such as in the event of detection of a serious compromise. For more information, see section 3.4.4.

4.10.7 Revocation checking requirement for Relying Parties

Relying parties shall check CRL's on a daily basis to ensure reliance on subscriber Certificates or if available, at any given point via the OCSP Responder as identified within each certificate in the chain.

4.10.8 CRL issuance frequency

The LAWtrust AeSign Certification Authority 2048 CRL issuance frequency is explained in section 3.4.4.

4.10.9 Maximum latency for CRL's

The maximum LAWtrust AeSign Certification Authority 2048 CRL latency is 7 days in the case where there are no revocations during that period.

4.10.10 On-line revocation/status checking availability

A Relying Party shall check whether the LAWtrust AeSign Certification Authority 2048 subscriber Certificate that the Relying Party wishes to rely on has been revoked. A Relying Party shall check the CRL maintained in the appropriate repository or via the appropriate OCSP Responder to determine whether the LAWtrust AeSign Certification Authority 2048 subscriber Certificate that the Relying Party wishes to rely on has been revoked. In no event shall LAWtrust or any Registration Authority operating under the LAWtrust AeSign Certification Authority 2048, or any sub-contractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable for any damages whatsoever due to:

1. The failure of a Relying Party to check the revocation or expiry of a LAWtrust AeSign Certification Authority 2048 subscriber Certificate; or

2. Any reliance by a Relying Party on a LAWtrust AeSign Certification Authority 2048 subscriber Certificate that has been revoked or that has expired.

3. Any reliance by a Relying Party on a LAWtrust AeSign Certification Authority 2048 subscriber Certificate that has been fraudulently used or used for the commission of fraudulent activities

4.10.11 On-line revocation checking requirements

A relying party must confirm the validity of a certificate in accordance with section 4.10.7 prior to relying on it or any cryptographic datum created using it.

4.10.12 Other forms of revocation advertisements available

The CRL in the LAWtrust repository contains the revoked certificates and these may be searched by their serial numbers.

The OCSP Responder service provides status information pertaining to a specified certificate serial number, submitted in the request. The service is available at http://ocsp.lawtrust.co.za.

4.10.13 Special requirements for key compromise

If a Subscriber suspects or knows that a private key corresponding with the public key contained in the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate has been compromised, the Subscriber shall immediately notify the LAWtrust AeSign Certificate Authority RA that processed the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate Application using the procedures set out in 4.10.3 of such suspected or actual compromise.

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

The Subscriber shall be responsible for investigating the circumstances of such compromise or suspected compromise and for notifying the LAWtrust AeSign Certification Authority 2048 and any Relying Parties that may have been affected by such compromise or suspected compromise.

4.10.14 Circumstances for suspension

A LAWtrust AeSign Certificate Authority RA may suspend a LAWtrust AeSign Certification Authority 2048 subscriber Certificate if the Subscriber is not in good standing with the LAWtrust AeSign Certification Authority 2048 or the LAWtrust AeSign Certificate Authority RA or the Subscriber fails to adhere to the provisions of this LAWtrust AeSign Certificate Authority 2048 CPS or the LAWtrust AeSign Certificate Authority RA Charter

4.10.14.1 Maximum number of allowed suspensions

There is no limit on the number of allowed suspensions a RA-Agent may place on a LAWtrust AeSign Certification Authority 2048 subscriber Certificate, except if this is specifically stated in the LAWtrust AeSign Certificate Authority RA Charter.

4.10.14.2 Who can request the lifting of a certificate suspension?

A LAWtrust AeSign Certificate Authority RA may request a LAWtrust AeSign Certification Authority 2048 to lift the suspension of a LAWtrust AeSign Certification Authority 2048 subscriber certificate without prior notice to the Subscriber. The LAWtrust AeSign Certificate Authority RA shall make a commercially reasonable effort to notify the Subscriber of the lifting of the suspension by sending an email, unless a different mechanism is specified in the LAWtrust AeSign Certificate Authority RA Charter, to the email address provided in the certificate application.

4.10.14.3 Procedure for the lifting of a suspension request

A LAWtrust AeSign Certificate Authority RA may request a LAWtrust AeSign Certification Authority 2048 to lift the suspension of a LAWtrust AeSign Certification Authority 2048 Subscriber Certificate in accordance with the provision of the LAWtrust AeSign Certificate Authority RA Charter as approved by the LAWtrust PA. This includes the process for bulk lifting of suspension requests.

4.10.14.4 Circumstances for lifting certificate suspension

A certificate is suspended if an event which may result in a revocation is suspected and not confirmed. If the evidence supporting the suspicion is later found to be invalid, then this would be grounds for lifting the suspension.

4.10.15 Who can request suspension

A LAWtrust AeSign Certificate Authority RA may request a LAWtrust AeSign Certification Authority 2048 to suspend a LAWtrust AeSign Certification Authority 2048 Subscriber Certificate without prior notice to the Subscriber. The LAWtrust AeSign Certificate Authority

RA shall make a commercially reasonable effort to notify the Subscriber of the suspension by sending an eMail, unless a different mechanism is specified in the LAWtrust AeSign Certificate Authority RA Charter, to the eMail address provided in the certificate application.

4.10.16 Procedure for suspension request

A LAWtrust AeSign Certificate Authority RA may request a LAWtrust AeSign Certification Authority 2048 to suspend a LAWtrust AeSign Certification Authority 2048 Subscriber Certificate in accordance with the provision of the LAWtrust AeSign Certificate Authority RA Charter as approved by the LAWtrust PA.

The LAWtrust AeSign Certification Authority 2048 receiving the suspension request shall, within a few minutes of performing the suspension, post the serial number of the suspended LAWtrust AeSign Certification Authority 2048 Subscriber Certificate to the CRL in the appropriate LAWtrust repository as specified in section 3.4.4.

If a Subscriber's LAWtrust AeSign Certification Authority 2048 certificate is suspended for any reason, the LAWtrust AeSign Certificate Authority RA that requested suspension of the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate shall make a commercially reasonable effort to notify the Subscriber by sending an email to the email address provided in the certificate application.

4.10.16.1 Procedure for bulk suspension request

A LAWtrust AeSign Certificate Authority RA may request the LAWtrust AeSign Certification Authority 2048 to suspend LAWtrust AeSign Certification Authority 2048 Subscriber certificates in bulk in accordance with the provision of the LAWtrust AeSign Certificate Authority RA Charter as approved by the LAWtrust PA.

The LAWtrust AeSign Certification Authority 2048 certificate administrator on receiving the bulk suspension request with the details of the Subscribers' accounts and LAWtrust AeSign Certification Authority 2048 Certificate serial numbers, shall prepare a list of certificate accounts to be send to the LAWtrust AeSign Certification Authority 2048 for bulk suspension.

The LAWtrust AeSign Certification Authority 2048 on receiving the bulk suspension request submitted by the LAWtrust certificate administrator, shall within a few minutes of performing the bulk suspension post the serial numbers of the suspended LAWtrust AeSign Certification Authority 2048 Certificates to the CRL in the appropriate LAWtrust repository as specified in section 3.4.4.

If the Subscribers' LAWtrust AeSign Certification Authority 2048 Certificates are suspended for any reason, the LAWtrust AeSign Certificate Authority RA that requested suspension of the Subscribers' certificates shall make a commercially reasonable effort to notify the Subscribers by sending an eMail to the eMail address provided in the certificate applications.

4.10.17 Limits on suspension period

A LAWtrust AeSign Certificate Authority RA may suspend a LAWtrust AeSign Certification Authority 2048 Certificate for a period not exceeding the validity of the certificate.

4.11 Certificate status services

4.11.1 Operational characteristics

The LAWtrust AeSign Certification Authority 2048 certificate status services make use of certificate revocation lists and online Certificate Status Protocol (OCSP) where appropriate.

4.11.2 Service availability

The LAWtrust AeSign Certification Authority 2048 certificate status services are available 24 hours a day, with reasonable time provided for maintenance.

4.11.3 Optional Features

The LAWtrust AeSign Certification Authority 2048 shall maintain a CRL at least every 24 (twenty-four) hours, with a minimum validity of 24 (twenty-four) hours.

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

The LAWtrust OCSP Responder service provides revocation status information in real time and is available 24 hours a day, with reasonable time provided for maintenance.

4.12 End of Subscription

The LAWtrust AeSign Certification Authority 2048 subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.13 Key escrow and recovery policy and practices

The LAWtrust AeSign Certification Authority 2048 will not provide a key escrow service.

4.13.1 Key Escrow and recovery policy and practices

No stipulation.

4.13.2 Session key encapsulation and recovery policy and practices

No stipulation.

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 of business activities and theft of information and information processing facilities.

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

5.1.1 Site Location and Construction

The LAWtrust AeSign Certification Authority 2048 hardware and software are hosted in a LAWtrust Vault at the hosted data center with physical security and access control procedures that meet or exceed industry standards.

5.1.2 Physical Access

Physical access to the LAWtrust AeSign Certification Authority 2048 is strictly controlled. Only authorised LAWtrust representatives may arrange to gain access to the CA's vault in the data center and they are identified by biometric access control.

All authorised personnel and all persons accompanying them under their authority need to sign an access register at the data centre Security Office. To access the LAWtrust AeSign Certification Authority 2048 at the data centre a minimum of two authorised LAWtrust representatives are required, one with the physical key and the biometric access control to the vault, and one with the physical key to access the rack where the CA's are hosted within the vault.

This access shall be logged and recorded by the data centre security personnel; all the relevant biometric readers and the LAWtrust AeSign Certification Authority 2048 vault access register.

5.1.2.1 Physical access systems testing

Where LAWtrust makes use of a third party to implement, manage and maintain physical access to LAWtrust CA facilities, LAWtrust shall implement testing of access systems or obtain evidence of the testing of such systems.

5.1.3 Power and Air Conditioning

The data centre shall be provided with power backup and air-conditioning.

5.1.4 Water Exposure

The hosted data centre is protected against water exposure.

5.1.5 Fire Prevention and Protection

The data center facility is fully wired for fire detection and alarm. Routine, frequent inspections of all systems are made to ensure 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 center.

5.2 Procedural Controls

The LAWtrust AeSign Certification Authority 2048 have a number of trusted roles for sensitive operations of the hardware and software used to facilitate the issue of certificates. Certification Authority operations related to adding administrative personnel or changing LAWtrust AeSign Certification Authority 2048 policy settings require more than one (1) person to perform the operation.

To gain access to the software used by the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 and require a high level of trust. A list of these roles is provided below.

5.2.1.1 LAWtrust AeSign Certification Authority 2048 Roles

- Administrator: Certificate lifecycle management tasks
- System Administrators: Administration of the operating system
- Cryptographic custodian: Person safekeeping cryptographic material.
- Witnesses: Persons performing witness roles of sensitive activities.
- First Officer: Security Officer as defined in the Entrust documentation
- Security Officer: Sensitive CA operations
- Entrust Master User 1, 2 and 3: start and stop CA services and other sensitive CA activities

5.2.1.2 Hardware Security Module Roles

5.2.1.2.1 HSM Administrator

The functions of the LAWtrust CA's HSM Administrator include:

- Provide login via SSH to Luna HSM
- Allows for copy and retrieval of certificates to and from the HSM

- Allows for certain functions to be performed on the HSM
- Provide first time login to the security functions of the HSM with the security officer
- Provide dual mechanisms on all security functions on the HSM

5.2.1.2.2 Security Officer (MofN)

The functions of the LAWtrust CA's HSM Security Officer include:

- Provide login to the security functions of the HSM
- Allows security functions to be performed on the HSM
- Provide first time activation of the partitions on the HSM

5.2.1.2.3 Cloning Domain User

The functions of the LAWtrust CA's HSM Cloning Domain User include:

- Allows for the backup and restore of HSM content to backup tokens and HSMs

5.2.1.2.4 Partition Owner

The functions of the LAWtrust CA's HSM Partition Owner include:

- Provide login to the partitions on the HSM
- Provide the partition password for all applications requiring access to specific partitions

5.2.2 Number of persons required per task

The CA's keys are only unencrypted in the FIPS 140-2 level 3 boundary of the HSM. To access the LAWtrust AeSign Certification Authority 2048 key material a minimum of three custodians are required. To keep the LAWtrust AeSign Certification Authority 2048 operational, the 3 of 6 scheme is loaded and kept persistent to allow the LAWtrust AeSign Certification Authority 2048 server access to the private key.

The activation of the LAWtrust AeSign Certification Authority 2048 key through the HSM requires three persons for the LAWtrust AeSign Certification Authority 2048. All roles are assigned strictly according to the prescriptions of the LAWtrust AeSign CA specifications.

5.2.3 Identification and authentication for each role

5.2.3.1 Luna Hardware Security Module Roles

Luna Hardware Security Module Roles

- HSM Admin role – 1 of 1
- HSM Security Officers – 3 of 6
- HSM Cloning Domain role – 1 of 1
- HSM Partition Owner Password– 1 of 1
- HSM Partition Owner PED / Password– 1 of 1

5.2.3.2 Operating system administrator Role

The access to the server operating systems is controlled by the domain controller.

5.2.3.3 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).

5.2.4 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 AeSign Certification Authority 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

The operational personnel for the 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 CA Policy
- Set or restore the CA Security Policy
- Sign LAWtrust Subordinate CA Certificates
- Import certificate definitions/specifications

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

5.3.1 Qualifications, experience and clearance requirements

LAWtrust personnel performing trusted roles and roles which support the operational infrastructure of the LAWtrust AeSign Certification Authority 2048 should;

1. be qualified via training certificate of competencies for the technologies in operation.
2. have at least one (1) year experience in configuration and supporting of the technologies in operation.
3. at a minimum have a background check performed when employed and when assigned a trusted role, thereafter at a frequency of at least every 2 years.

5.3.2 Background Check and Clearance Procedures

The LAWtrust on boarding process includes the following background checks:

- Employment Reference check;
- Education certificates check;
- Criminal Check;

5.3.3 Training Requirements And Procedures

LAWtrust personnel performing trusted roles and roles which support the operational infrastructure of the LAWtrust AeSign Certification Authority 2048 should attend training on the following:

- Underlying hardware infrastructure for server hardware;
- Operating systems;
- Applications used in the LAWtrust AeSign Certification Authority 2048 operations;
- Hardware Security Modules;

5.3.4 Retraining Frequency and Requirements

LAWtrust Personnel should be retrained when a new version of software or underlying hardware platform is being planned for operations or every two years whichever is realised first.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation

5.3.6 Sanctions for Unauthorized Actions

Non-Compliance with this CPS by any LAWtrust employee, either through negligence or malicious intent, will be subject to the LAWtrust disciplinary procedure, which may result in termination of employment. Non-Compliance with this CPS by a LAWtrust appointed RA either through its contractors or employees may lead to the suspension or termination of the RA's appointment as an RA and any person found responsible may be subject to criminal charges.

5.3.7 Independent contractor requirements

Independent contractors are required to undergo the same process as full-time employees.

- Independent contractor agreement
- Adhere to the LAWtrust Information Security Policies and Procedures.

- No independent contractor will be assigned to a trusted role.

5.3.8 Documentation Supplied to Personnel

LAWtrust personnel will have access to the following documentation

- LAWtrust information Security Policies
- Information Security awareness training material

5.4 Audit Logging Procedures

Significant security events in the LAWtrust AeSign Certification Authority 2048 is automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Only authorised CA personnel and authorised RA personnel operating under the LAWtrust AeSign Certification Authority 2048 can view the audit trail files.

The integrity of the audit files is protected against modification. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archiving facility.

5.4.1 Types of events recorded

The CA maintains controls to provide reasonable assurance that:

1. significant CA environmental, key management, and certificate management events are accurately and appropriately logged;
2. the confidentiality and integrity of current and archived audit logs are maintained;
3. audit logs are completely and confidentially archived in accordance with disclosed business practices; and
4. audit logs are reviewed periodically by authorized personnel.

The authentication (failure and success) of all operational staff assigned trusted roles is recorded in an audit trail. This applies to unique username and password and certificate authentication.

The following table includes events that are considered to be of sufficient significance to be entered into the Audit trail.

Category	Description events, audit log and process
Audit Logs	1 The CA generates automatic (electronic) and manual audit logs in accordance with the requirements of the CP and/or CPS.
	2 All journal entries include the following elements:
	a) date and time of the entry;
	b) serial or sequence number of entry (for automatic journal entries);
	c) kind of entry;
	d) source of entry (e.g., terminal, port, location, customer, etc.); and
	e) identity of the entity making the journal entry.
Events Logged	3 The CA logs the following CA and subscriber (if applicable) key life cycle management related events:
	a) CA key generation;
	b) installation of manual cryptographic keys and its outcome (with the identity of the operator);
	c) CA key backup;
	d) CA key storage;
	e) CA key recovery;
	f) CA key escrow activities (if applicable);
	g) CA key usage;
	h) CA key archival;
	i) withdrawal of keying material from service;

Category	Description events, audit log and process
	j) CA key destruction;
	k) identity of the entity authorizing a key management operation;
	l) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media);
	m) custody of keys and of devices or media holding keys; and
	n) compromise of a private key.
	4 The CA logs the following cryptographic device life cycle management related events:
	a) device receipt and installation;
	b) placing into or removing a device from storage;
	c) device activation and usage;
	d) device de-installation;
	e) designation of a device for service and repair; and
	f) device retirement.
	5 If the CA provides subscriber key management services, the CA logs the following subscriber key life cycle management related events:
	a) key generation;
	b) key distribution (if applicable);
	c) key backup (if applicable);
	d) key escrow (if applicable);
	e) key storage;
	f) key recovery (if applicable);
	g) key archival (if applicable);
	h) key destruction;

Category	Description events, audit log and process
	i) identity of the entity authorizing a key management operation; and
	j) key compromise.
	6 The CA records (or requires that the RA record) the following certificate application information:
	a) the method of identification applied and information used to meet subscriber requirements;
	b) record of unique identification data, numbers, or a combination thereof (e.g., applicants driver's license number) of identification documents, if applicable;
	c) storage location of copies of applications and identification documents;
	d) identity of entity accepting the application;
	e) method used to validate identification documents, if any;
	f) name of receiving CA or submitting RA, if applicable;
	g) the subscriber's acceptance of the Subscriber Agreement; and
	h) where required under privacy legislation, the Subscriber's consent to allow the CA to keep records containing personal data, pass this information to specified third parties, and publication of certificates.
	7 The CA logs the following certificate life cycle management related events:
	a) receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests;
	b) submissions of public keys for certification;
	c) change of affiliation of an entity;
	d) generation of certificates;
	e) distribution of the CA's public key;
	f) certificate revocation requests;
	g) certificate revocation;

Category	Description events, audit log and process
	h) certificate suspension requests (if applicable);
	i) certificate suspension and reactivation; and
	j) generation and issuance of Certificate Revocation Lists.
	8 The CA logs the following security-sensitive events:
	a) security-sensitive files or records read or written including the audit log itself;
	b) actions taken against security-sensitive data;
	c) security profile changes;
	d) use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts);
	e) system crashes, hardware failures and other anomalies;
	f) actions taken by individuals in Trusted Roles, computer operators, system administrators, and system security officers;
	g) change of affiliation of an entity;
	h) decisions to bypass encryption/authentication processes or procedures; and
	i) access to the CA system or any component thereof.
	9 Audit logs do not record the private keys in any form (e.g., plaintext or enciphered).
	10 CA computer system clocks are synchronized for accurate recording as defined in the CP and/or CPS that specifies the accepted time source.
Audit Log Protection	11 Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorized destruction.
	12 Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.
	13 The private key used for signing audit logs is not used for any other purpose. This applies equally to a symmetric secret key used with a symmetric MAC mechanism.
	14 The CA archives audit log data on a periodic basis as disclosed in the CP and/or CPS.

Category	Description events, audit log and process
Audit Log Archival	15 In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.
	16 The CA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.
	17 Current and archived audit logs are only retrieved by authorized individuals for valid business or security reasons.
Review of Audit Logs	18 Audit logs are reviewed periodically according to the practices established in the CPS. The review of current and archived audit logs includes a validation of the audit logs' integrity, and the timely identification and follow up of unauthorized or suspicious activity.

Table 1: Audit Log requirements

5.4.2 Frequency of Processing Log

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 PKI audit logs are retained for a period as stipulated in section 5.5.1.1

5.4.4 Protection of Audit Log

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

The information 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

Audit Logs are backed up daily and moved from the CA to the onsite NAS and then to the offsite NAS.

5.4.6 Audit Collection System (Internal or External)

Audit Logs are backed up daily and retained for seven (7) years.

5.4.7 Notification to Event-Causing Subject

No Stipulation

5.4.8 Vulnerability Assessments

The LAWtrust AeSign Certification Authority 2048 operational environment will have regular vulnerability assessments performed.

5.5 Records Archival

5.5.1 Types of records archived

The LAWtrust AeSign Certification Authority 2048 will retain the following relevant information with respect to the PKI operations. The records included will at a minimum include;

5.5.1.1 Digital Certificate lifecycle records

1. Applications for the issuing of digital certificates
2. Registration and verification documents for certificates issued
3. Information related to suspended certificates
4. Information Related to expired and revoked certificates

5.5.1.2 Digital certificate Validation records

Certificate repository is maintained in a manner that subscribers and relying parties can readily access records to which LAWtrust permit access.

5.5.1.3 PKI Operational Records

Reliable records in the form of log files and audit trails of activities that are core to the PKI operations including:

1. certificate management,
2. encryption key generation, and
3. administration of computing facilities.

5.5.1.4 PKI Database records

All databases for the LAWtrust AeSign Certification Authority 2048 are encrypted and protected by the LAWtrust AeSign Certification Authority 2048 master keys. Archive files are backed up according to a daily backup schedule provided at the data centre. Archive files are stored at a secure and separate geographic location.

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 AeSign Certification Authority 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

Electronic archives are protected in a manner which allows the integrity of the archive to be verified at a later point.

5.5.4 Archive Backup Procedures

Audit Logs remain on the CA file system until the files are moved to the onsite NAS.

5.5.5 Requirements for Time-Stamping of Records

Electronic records are timestamped using the current date and time of each event associated with that record, using the system time.

5.5.6 Archive Collection System (Internal or External)

All information included in the LAWtrust archives are collected by LAWtrust internal systems.

5.5.7 Procedures to Obtain and Verify Archive Information

A formal, written request can be made to the LAWtrust PA to gain access to the Archives for disciplinary and or legal proceedings. The LAWtrust PA in consultation with the LAWtrust Security Committee will review the request and provide a decision to the requestor in writing within 7 (seven) working days of the request. The decision communicated to the requestor will be final.

5.6 Key Changeover

Subscribers are issued LAWtrust AeSign Certification Authority 2048 Certificates that 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 Certificate Application to replace an expiring LAWtrust AeSign Certification Authority 2048.

LAWtrust AeSign Certification Authority 2048 key pair will be retired from service at the end of their respective lifetimes as defined in section 6.3.2. New CA key pairs will be created as required to support the continuation of LAWtrust AeSign Certification Authority 2048 Services.

The LAWtrust AeSign Certification Authority 2048 will continue to publish CRLs signed with the original key pair until all certificates issued using that original key pair have expired. The CA key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

5.7 Compromise and Disaster Recovery

The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048. The compromise of the private key used by the LAWtrust AeSign Certification Authority 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.

5.7.1 Incident and compromise handling procedures

LAWtrust AeSign Certification Authority 2048 maintain incident response procedures to provide appointed stakeholders guidance in responding to, containing, investigating and restoration of systems exposed to information security incidents.

5.7.2 Computing resources, software, and/or data are corrupted

LAWtrust AeSign Certification Authority 2048 maintain daily backups for the purposes of recovering from data, software and or computing system corruption. The LAWtrust Disaster Recovery procedures cover the recovery in the case of corruption.

5.7.3 Entity private key compromise procedures

In the case of an entity private key loss or compromise, LAWtrust AeSign Certification Authority 2048 will follow the LAWtrust Incident Response Procedures.

5.7.4 Business continuity capabilities after a disaster

Post recovery from a disaster, LAWtrust systems will be switched over to the production environment.

5.8 LAWtrust AeSign Certification Authority 2048 or LAWtrust AeSign Certificate Authority RA termination

In the event that a LAWtrust AeSign Certificate Authority RA ceases operation, all LAWtrust AeSign Certification Authority 2048 Certificates issued by the appointed LAWtrust AeSign Certificate Authority RA will be revoked.

In the event that the LAWtrust AeSign Certification Authority 2048 ceases operation, the LAWtrust AeSign Certification Authority 2048 Certificate will be revoked by the LAWtrust Root Certification Authority 2048. If LAWtrust believes that there is a risk that the specific LAWtrust AeSign Certification Authority 2048 private key has been compromised, then LAWtrust will immediately inform LAWtrust AeSign Certificate Authority RAs and Subscribers of such a compromise. LAWtrust shall also notify providers of software applications who distributes such CA keys of such a termination and resulting revocation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

The signing key pair for the LAWtrust AeSign Certification Authority 2048 was created during the initial start-up of the LAWtrust AeSign Certification Authority 2048 and are protected by the master keys for the LAWtrust AeSign Certification Authority 2048. Hardware key generation is used which is compliant to FIPS 140-2 level 3 for the LAWtrust AeSign Certification Authority 2048 and uses FIPS 186-2 key generation techniques.

6.1.1 Key pair generation

The subscriber private key or SCD is always generated within a SSCD as specified by the subscriber requirements. The SSCD's are provided by means of FIPS 140-2 rated Hardware Tokens.

6.1.2 Private key delivery to Subscriber

The subscriber private key is always generated under the sole control of the subscriber/applicant within a SSCD.

The Applicant shall be responsible for the generation and safeguarding of private keys unless otherwise required in terms of a LAWtrust AeSign RA Charter as approved by the LAWtrust PA

6.1.3 Public key delivery to certificate issuer

The public key to be included in a LAWtrust AeSign CA Certificate is delivered to the LAWtrust AeSign CA in a Certificate Signing Request (CSR) as part of the LAWtrust Certificate Application process.

6.1.4 CA public key delivery to Relying Parties

The LAWtrust Root Certification Authority 2048 and the LAWtrust AeSign Certification Authority 2048 public keys are available on the LAWtrust repository using the following url:

https://www.lawtrust.co.za/repository

6.1.5 Key Sizes

The minimum key size for any LAWtrust AeSign Certification Authority 2048 issued certificate is 2048-bit RSA. Currently the LAWtrust AeSign Certification Authority 2048 has a key size of 2048-bit RSA.

The LAWtrust PA will perform an annual review on the LAWtrust AeSign Certification Authority 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

LAWtrust AeSign Certification Authority 2048uses FIPS 140-2 hardware security modules which provides random number generation and all cryptographic keys are generated in the SSCD formats stipulated in section 6.1.1.

6.1.7 Key Usage Purposes

LAWtrust AeSign CA Certificates issued by the LAWtrust AeSign CA contain the key usage and extend usage certificates and extensions restricting the purpose for which the LAWtrust AeSign CA Certificate can be used.

The Key Usage for end user certificates will be for

1) Digital Signature,
2) Non Repudiation
3) Key Encipherment (a0)

Subscribers and Relying Parties shall only use LAWtrust AeSign CA Certificates in compliance with this LAWtrust AeSign Certificate Authority 2048 CPS and applicable laws.

6.2 Private Key Protection and Crypto-Module Engineering Controls

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

6.2.1 Cryptographic Module Standards and Controls

LAWtrust AeSign Certification Authority 2048 provides assurance that all hardware security modules used are FIPS 140-2 rated.

6.2.2 CA Private Key Multi-Person Control

Multi-person control of the LAWtrust AeSign Certification Authority 2048 private key is achieved using an “m-of-n” split key knowledge scheme. LAWtrust AeSign Certification Authority 2048 keys can only be accessed on the physical and logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.

6.2.3 Private Key Escrow

LAWtrust AeSign Certification Authority 2048 does not provide subscriber key escrow.

6.2.4 Private Key Backup

All LAWtrust AeSign Certification Authority 2048 private keys are generated and stored by the approved hardware security modules. All backup keys are for Business Continuity requirements and are stored with the same level of protection as keys in production.

6.2.5 Private Key Archival

The LAWtrust AeSign Certification Authority 2048 does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

LAWtrust AeSign Certification Authority 2048 private keys are not transferred out of hardware security modules.

6.2.7 Private Key Storage on Cryptographic Module

The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 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 AeSign Certification Authority 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

LAWtrust AeSign Certification Authority 2048 destroy private keys using guidelines provided by the manufacturer of the hardware security module. Where key shares are stored on smartcards, the smartcards are destroyed in a scripted and witnessed ceremony.

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 AeSign Certification Authority 2048 certificate (which contains the public key) is backed up and archived as part of the LAWtrust AeSign Certification Authority 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:

Certificate	Private Key use	Certificate valid until
Root CA: LAWtrust Root CA	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	16 May 2032 06:10:18 PM
Issuing CA: LAWtrust AeSign Certification Authority 2048	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	15 January 2030 11:22:03 AM
CRL Signing Certificate:	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
OCSP Signing Certificate:	critical Digital Signature, Extended Key Usage: critical OCSP Signing	
End Entity Certificates Signing	Digital Signature, Non-Repudiation (c0)	Not after 15 January 2030

6.4 Activation Data

All LAWtrust AeSign Certification Authority 2048 private keys are activated according to the manufacturer's requirements. The detailed activities are scripted and witnessed by at least six trusted personnel.

6.4.1 Activation Data Generation and Installation

All LAWtrust AeSign Certification Authority 2048 private key activation data is protected using vendor specific controls together with personnel and physical security controls. (use of trusted employees, Accounts lockout on multiple authentication failures, key shares are distributed among multiple trusted employees.

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 AeSign Certification Authority 2048. 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

6.5.1 Specific Computer Security Technical Requirements

The servers on which the LAWtrust AeSign Certification Authority 2048 operate are physically secured as described in 5.1 of this LAWtrust AeSign Certificate Authority 2048 CPS. The operating systems on the servers on which LAWtrust AeSign Certification Authority 2048 operate enforce identification and authentication of users. Access to LAWtrust AeSign Certification Authority 2048 software databases and audit trails is restricted as described in this LAWtrust AeSign Certificate Authority 2048 CPS.

All operational personnel that are authorised to have access to the LAWtrust AeSign Certification Authority 2048 is required to use a physical key in conjunction with a biometric authentication to gain access to the secure vault that hosts the LAWtrust AeSign Certification Authority 2048. Physical access to the data centre that hosts the secure vault where the LAWtrust AeSign Certification Authority 2048 equipment and LAWtrust AeSign Certification Authority 2048 software are located is described in 5.1.2.

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 AeSign Certification Authority 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 utilise approved commercial products for the core PKI components.

6.6.2 Security Management Controls

LAWtrust maintains a configuration of the PKI and any changes to that configuration is documented in the LAWtrust Change Management Process.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The LAWtrust AeSign Certification Authority 2048 hosted in the LAWtrust vault will operate on a dedicated network segment and access to the LAWtrust AeSign Certification Authority 2048's hardware and software is protected by firewall and intrusion detection. The virus and other malicious software detection and prevention tools as described in the LAWtrust Information Security Policy will be installed on all LAWtrust AeSign Certification Authority 2048 servers.

6.8 Time Stamping

LAWtrust PKI systems time is synchronised to a local trusted time source. System time is set to SAST. The accuracy of system time is within one second.

6.9 Information security

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

6.10 Escalation of information security violations

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

6.11 Secure communication between the RA and the CA

It is a requirement for all digital certificate lifecycle events to be secure, as such all communication between the RA and the CA will be secured in the following manner

1. TLS protecting communications between administrator's authentication to the RA.
2. Only administrators identified by the RA and authorised by LAWtrust will be provisioned with access to the RA.

All digital certificate lifecycle events will be protected in this manner, account creation, certificate issuance, suspension, revocation etc.

6.12 Security Management

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

PKI, Certificate Authority Specific Polices (Including Certificate Policy, Certificate Practice Statement and Registration Authority Charters)

Information Security Polices (Including the specific policies as stipulated in the LAWtrust Information Security Policy in support of the PKI Practices).

6.12.1 CA key pair usage

The LAWtrust AeSign Certification Authority 2048's private signing keys are used for signing LAWtrust AeSign Certification Authority 2048 Certificates and Certificate Revocation Lists exclusively.

7. CERTIFICATE, CRL, OCSP AND SYSTEM CERTIFICATE 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 AeSign Certification Authority 2048 is described in the LAWtrust PKI Certificate Profiles document, an internal LAWtrust Operational document.

7.1.1 Version Numbers

LAWtrust AeSign Certification Authority 2048 shall issue X.509 v3 certificates.

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.

7.1.2 Certificate Extensions

Table 2

Field Type	Field Name	Value format	Value	Explanation
	Authority Information Access	URL	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.lawtrust.co.za [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ltadss.lawtrust.co.za/certs/aesignica.cer[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.lawtrust.co.za	The authority information access extension indicates how to access information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data.
	Certificate Policies	URL	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.54383.1.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.lawtrust.co.za/repository [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=LAWtrust issues Certificates to subscribers as outlined by the LAWtrust Certification Practice Statement (CPS) which can be found at https://www.lawtrust.co.za/repository.	The LAWtrust documentation governing the CA and certificate usage is published at https://www.lawtrust.co.za/repository. The documentation set includes Policies, Practices and Agreements
Certificate Extensions	CRL Distribution Points	URL	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_c	The LAWtrust AeSign Certification Authority 2048 will issue CRLs and make them available via

Field Type	Field Name	Value format	Value	Explanation
			a_crlfile.crl	1] http at http://aesigncrl.lawtrust.co.za. The CA will issue at least one crl publication by the end of each business day.
	Authority Key Identifier		KeyID=5d2a63d08935c684a1b19a74c49a18c3070903ea	The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number.
	Subject Key Identifier		KeyID=5d2a63d08935c684a1b19a74c49a18c3070903ea (Sample)	The Subject Key Identifier is used by path validation software by helping to identify certificates that contain a particular public key. This is unique on each certificate
	Basic Constraints		Subject Type=End Entity Path Length Constraint=None	Constraints description
	Thumbprint			The digest (or thumbprint) of the certificate data.
	Key Usage		Digital Signature, Non-Repudiation or Key Encipherment	
	Enhanced Key Usage			

7.1.3 Algorithm Object Identifiers

LAWtrust certificates are signed using one of the following algorithms

Field Type	Field Name	Value format	Value	Explanation
X.509 Fields	Signature Algorithm	SHA2/RSA	SHA256	Algorithm to produce signatures
	Signature hash algorithm	Sha2	SHA256	
	Thumbprint Algorithm	sha2	SHA256	

- Note: Any certificates issued before the release date of this version of the CPS could have a signature algorithm of SHA1.

7.1.4 Name Forms

Certificates issued by LAWtrust AeSign Certification Authority 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

Field Type	Field Name	Value format	Value	Explanation
OID	Certificate Policies	text	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.54383.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.lawtrust.co.za/repository	

7.1.7 Usage of Policy Constraints Extension

Field Type	Field Name	Value format	Value	Explanation
	Basic Constraints	text	Subject Type=End Entity Path Length Constraint=None	

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No Stipulation

7.2 CRL Profile

7.2.1 Version number(s)

Version: set to v2

7.2.2 LAWtrust AeSign Certification Authority 2048 CRL Extensions

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

Field Type	Field Name	Value format	Value	Explanation
	Version	text	V2	
	Issuer		CN=LAWtrust AeSign Certification Authority 2048, OU=LAW Trusted Third Party Services PTY Ltd.,O=LAWtrust,C=ZA	
	Effective date		Time of current CRL issuance	

Field Type	Field Name	Value format	Value	Explanation
	Next update		Time of next expected CRL issuance	
	Signature algorithm		SHA256 RSA	
	Signature hash algorithm		SHA256	
extension	CRL number		unique 32-bit non-negative integer	
extension	Authority key identifier		20 byte SHA-2 hash of the Issuer's public key	
	Revoked certificates		List of serial numbers of revoked certificates	
	Issuer Signature		Digital Signature	

7.3 OCSP Profile

7.3.1 Version Number

The LAWtrust OCSP Server is an advanced x.509 certificate Validation Authority server. It is compliant with IETF RFC 2560, Online Certificate Status Protocol (OCSP) version 1.0

7.3.2 OCSP Extensions

No stipulation.

7.4 System Certificate Profiles

7.4.1 Purpose of Certificate

System certificates are used for authentication between various front-end systems and the CA to establish a secure channel.

7.4.2 Extensions

No Stipulation

8. Compliance Audit and Other Assessments

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

- LAWtrust AeSign Certification Authority 2048 Business Practices Disclosure;
- Service Integrity;
- LAWtrust AeSign Certification Authority 2048 Environmental Controls.

8.1 Frequency of Audit or Assessments

The LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 shall be independent from the Entity being audited.

8.4 Topics Covered By Assessment

The compliance audit shall test compliance of the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 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

9.1.1 Certificate issuance or renewal fees

The fees for services provided by LAWtrust in respect to LAWtrust AeSign Certification Authority 2048 Certificates are set forth in the LAWtrust Fees Schedule and information on these fees can be obtained from LAWtrust through contact details supplied in the LAWtrust Repository. These fees are subject to change, and any such changes shall become effective immediately after changing the Fees Schedule and posting the notice of changes in the

LAWtrust Repository. The fees for services provided by independent third-party Registration Authorities, Resellers and Co-marketers in respect to LAWtrust AeSign Certification Authority 2048 Certificates are set forth in Fees Schedules maintained by such Registration Authorities, Resellers and Co-marketers. These fees are subject to change, and any such changes shall become effective immediately after changing the Fees Schedules and notification to effected parties.

9.1.2 Certificate access fees

LAWtrust do not publish certificate access fees on their website.

9.1.3 Revocation or status information access fees

LAWtrust do not publish certificate revocation or status fees on their website.

9.1.4 Fees for other services

LAWtrust does not charge a fee for access to the LAWtrust CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a licence agreement with the party holding the copyright to the document.

9.1.5 Refund policy

1. Should a LAWtrust client be dissatisfied with a purchase and informs LAWtrust within 20 working days from date of purchase, a full refund will be issued less administration fees of 5%.
2. This policy will not apply to bulk purchases or purchases entered into between LAWtrust and another legal entity.
3. LAWtrust will always treat personal information with the greatest respect and security and also do not share personal information with anyone, except those parties that are required to have access to personal information in order to ensure the processing of your transaction, which parties include our payment gateway partner and any third-

party vendor whose products we resell. The LAWtrust privacy notice may be accessed at https://www.altron.com/policies/privacy-policy/.

4. These terms and conditions are in addition to the LAWtrust Standard Terms and Conditions, accessible at https://www.lawtrust.co.za/pages/terms-and-conditions and any other agreement entered into between you and LAWtrust.
5. In the event of a conflict between the terms of this Agreement and the other agreements referred to in clause 4 above, the provisions of this Agreement, will prevail only where such other agreement is silent on the issue of refunds and returns.

9.2 Financial Responsibility

9.2.1 Insurance coverage

LAWtrust has sufficient insurance in place to provide coverage for its responsibilities in terms of this CPS. The insurance in place covers:

- General Liability
- Professional Indemnity
- Cyber Liability
- Directors and Officers Liability

9.2.2 Other assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of business information

LAWtrust will not use, disclose or sell Applicant or Subscriber information, except in accordance with this LAWtrust AeSign Certificate Authority 2048 CPS, Subscriber Agreement

or Relying Party Agreement. LAWtrust and LAWtrust AeSign Certificate Authority RA shall use commercially reasonable care to prevent such information from being used or disclosed for purposes other than those described in this LAWtrust AeSign Certificate Authority 2048 CPS, Subscriber's Agreement or Relying Party Agreement. Notwithstanding the foregoing Applicants and Subscribers acknowledge that some of the information supplied with a LAWtrust AeSign Certification Authority 2048 Certificate Application is incorporated into a LAWtrust AeSign Certification Authority 2048 Certificate and that the LAWtrust AeSign Certification Authority 2048, LAWtrust AeSign Certificate Authority RA 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 AeSign Certification Authority 2048 Certificate, and which is not included in the information described in 9.3.2 below, shall be considered to be confidential. The LAWtrust AeSign Certification Authority 2048 and LAWtrust AeSign Certificate Authority RA's 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 AeSign Certification Authority 2048 Certificate Applications or that are assisting LAWtrust in the operation of the LAWtrust AeSign Certification Authority 2048 or LAWtrust AeSign Certificate Authority RA's. 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 AeSign Certification Authority 2048 and LAWtrust AeSign Certificate Authority RA's 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.

9.3.2 Information not within the scope of confidential information

Information that is included in a LAWtrust AeSign Certification Authority 2048 Certificate or a LAWtrust Revocation List shall not be considered confidential.

Information contained in this LAWtrust AeSign Certificate Authority 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, the LAWtrust AeSign Certification Authority 2048 or the LAWtrust AeSign Certificate Authority RA's;
- Was rightfully known or becomes rightfully known to the LAWtrust AeSign Certification Authority 2048 or a LAWtrust AeSign Certificate Authority RA without confidential or proprietary restriction from a source other than the Subscriber;
- Is independently developed by LAWtrust or a LAWtrust AeSign Certificate Authority RA; or
- Is approved by a Subscriber for disclosure.

9.3.3 Responsibility to protect confidential information

LAWtrust, and LAWtrust AeSign Certificate Authority RA's shall use commercially reasonable care to prevent such confidential information from being used or disclosed for purposes other than set out in this LAWtrust AeSign Certificate Authority 2048 CPS, Subscriber Agreements 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

LAWtrust is guided by its Privacy Notice found as per section 9.4. Information is only disclosed to authorised bodies of law enforcement and or to the owner of the information. If there is a need for personal information to be disclosed, the person who is the owner of the information will be approached to provide consent.

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

LAWtrust, its employees, contractors and appointed RA's are expected to treat all private information in accordance with the LAWtrust Privacy Policy. Subscriber information which is published in a digital certificate and or in certificate status mechanisms is done so with the consent of the subscriber.

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

LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under the CPS and all Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in a Certificate, which information shall remain the property of the Applicant or Subscriber.

9.6 Representations and Warranties

9.6.1 LAWtrust AeSign Certification Authority 2048 Representations and Warranties

LAWtrust makes the following limited warranties with respect to the operation of LAWtrust AeSign Certification Authority 2048:

- LAWtrust AeSign Certification Authority 2048 shall provide Repository services consistent with the practices and procedures set forth in the LAWtrust AeSign Certification Authority 2048 CPS;
- LAWtrust AeSign Certification Authority 2048 shall perform LAWtrust AeSign Certification Authority 2048 Certificate issuance consistent with the procedures set forth in this LAWtrust AeSign Certificate Authority 2048 CPS; and
- LAWtrust AeSign Certification Authority 2048 shall provide revocation services consistent with the procedures set forth in the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 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 AeSign Certification Authority 2048 Certificate,

- Any software whatsoever, or

- Non-repudiation of any LAWtrust AeSign Certification Authority 2048 Certificate or any transaction facilitated through the use of a LAWtrust AeSign Certification Authority 2048 Certificate, since such determination is a matter of applicable law.

- Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to LAWtrust AeSign Certification Authority 2048 Certificates and application using LAWtrust AeSign Certification Authority 2048 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 AeSign Certificate Authority RA or the employees, or directors of LAWtrust or a LAWtrust AeSign Certificate Authority RA. Neither LAWtrust nor any LAWtrust AeSign Certificate Authority RA or employees, or directors of LAWtrust or a LAWtrust AeSign Certificate Authority RA, shall be liable for any error, failure, delay, interruption, defect, or corruption in relation to a LAWtrust AeSign Certification Authority 2048 Certificate, a LAWtrust AeSign Certification Authority 2048 Certificate CRL, OCSP Response or a LAWtrust AeSign Certification Authority 2048 Certificate Application to

the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

9.6.2 CA representations and warranties

The same liability provisions that apply in Section 9.6.1 with respect to LAWtrust AeSign Certification Authority 2048 shall apply with respect to LAWtrust AeSign Certificate Authority RA's and employees, and directors of the foregoing.

9.6.3 RA Representations and Warranties

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

9.6.4 Relying Parties Representations and Warranties

Relying Parties represent and warrant to LAWtrust that:

- All information provided by the Subscriber or Applicant to LAWtrust or to a LAWtrust AeSign Certificate Authority RA is correct and does not contain any errors, omissions, or misrepresentations;
- Where applicable, the private key corresponding to the public key submitted by the Applicant or Subscriber in connection with a LAWtrust AeSign Certification Authority 2048 Certificate Application was created using sound cryptographic techniques and has not been compromised;
- Any information provided to LAWtrust or to a LAWtrust AeSign Certificate Authority RA by the Applicant or Subscriber in connection with a LAWtrust AeSign Certification Authority 2048 Certificate Application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;

- The Applicant shall notify the LAWtrust AeSign Certificate Authority RA to which it submitted a certificate application as soon as practicable if any information included in the Applicant's LAWtrust AeSign Certification Authority 2048 Certificate Application changes or if any change in any circumstances would make the information in the Applicant's LAWtrust AeSign Certification Authority 2048 Certificate Application misleading or inaccurate;

- The Subscriber shall immediately cease to use the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate if any information included in the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate changes or if any change in any circumstances would make the information in the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate misleading or inaccurate;

- The Subscriber shall immediately cease to use the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate upon:

    - Expiration, suspension or revocation of the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate, or

    - Any suspected or actual compromise of the private key corresponding to the public key in such LAWtrust AeSign Certification Authority 2048 Certificate, and shall remove such LAWtrust AeSign Certification Authority 2048 Certificate from the devices and/or software in which it has been installed.

- The Subscriber and/or Applicant Shall not use LAWtrust AeSign Certification Authority 2048 Certificates for any hazardous or unlawful (including tortuous) activities.

9.6.5 Subscriber Representations and Warranties

Subscribers and Applicants represent and warrant to LAWtrust that:

- All information provided by the Subscriber or Applicant to LAWtrust or to a LAWtrust AeSign Certificate Authority RA is correct and does not contain any errors, omissions, or misrepresentations;

- Where applicable, the private key corresponding to the public key submitted by the Applicant or Subscriber in connection with a LAWtrust AeSign Certification Authority 2048 Certificate Application was created using sound cryptographic techniques and has not been compromised;
- Any information provided to LAWtrust or to a LAWtrust AeSign Certificate Authority RA by the Applicant or Subscriber in connection with a LAWtrust AeSign Certification Authority 2048 Certificate Application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;
- The Applicant shall notify the LAWtrust AeSign Certificate Authority RA to which it submitted a certificate application as soon as practicable if any information included in the Applicant's LAWtrust AeSign Certification Authority 2048 Certificate Application changes or if any change in any circumstances would make the information in the Applicant's LAWtrust AeSign Certification Authority 2048 Certificate Application misleading or inaccurate;
- The Subscriber shall immediately cease to use the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate if any information included in the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate changes or if any change in any circumstances would make the information in the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate misleading or inaccurate;
- The Subscriber shall immediately cease to use the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate upon:
    - Expiration, suspension or revocation of the Subscriber's LAWtrust AeSign Certification Authority 2048 Certificate, or
    - Any suspected or actual compromise of the private key corresponding to the public key in such LAWtrust AeSign Certification Authority 2048 Certificate, and shall remove such LAWtrust AeSign Certification Authority 2048 Certificate from the devices and/or software in which it has been installed.

- The Subscriber and/or Applicant Shall not use LAWtrust AeSign Certification Authority 2048 Certificates for any hazardous or unlawful (including tortuous) activities.

9.6.6 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimers of Warranties

Except as specifically provided in sections 9.5 and 0, neither LAWtrust, the LAWtrust AeSign Certification Authority 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

By relying on any certificate issued in terms of the provisions of this CPS you fully indemnify LAWtrust, any hardware and any other parties whose products are utilised in the certificate lifecycle chain. This indemnity includes indemnification against any losses of whatsoever nature, in whatever jurisdiction you may suffer as a result of your use of or reliance on a digital certificate.

9.10 Term and Termination

9.10.1 Term

This CPS is effective when published to the LAWtrust repository. Newer versions will replace any superseded versions.

9.10.2 Termination

This CPS remains in effect until replaced.

9.10.3 Effect of Termination and Survival

CPS termination impact and following management proceeding will be communicated via the appointed RA's or via the LAWtrust repository.

9.11 Individual Notices and Communications with Participants

Unless expressly agreed with any participant to the contrary in writing, or stipulated by the LAWtrust PA to the contrary, communications addressed to a participant by LAWtrust, the LAWtrust AeSign Certification Authority 2048 or a LAWtrust AeSign Certificate Authority RA may, at the foregoing discretion, be communicated by eMail to the eMail address provided by the participant.

9.12 Amendments

9.12.1 Process for amendments

- LAWtrust PA shall consider the provisions of this LAWtrust AeSign Certificate Authority 2048 CPS, any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or LAWtrust AeSign Certificate Authority RA Charter, previously approved by at least annually and shall also consider proposals for amendment that may be received from the LAWtrust OA or a LAWtrust AeSign Certificate Authority RA.
- A proposal for an amendment to this LAWtrust AeSign Certificate Authority 2048 CPS or to any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or LAWtrust AeSign Certificate Authority RA Charter, previously approved by the LAWtrust PA shall be submitted to the LAWtrust PA for consideration.
- The LAWtrust PA shall within a period of not more than 60 (sixty) days from the date of receipt of the proposal, consider the proposal and determine whether the proposal for amendment well founded and an amendment warranted.
- Once an amendment has been drafted it shall be considered by the LAWtrust PA taking into account good practice relating to the PKI, information security and the needs and best interests of the participants to the PKI.

9.12.2 Notification mechanism and period

- The LAWtrust PA shall determine the notification mechanisms and period before which an amendment may become effective in each instance and may provide written directives in this regard.
- The LAWtrust PA shall exercise reasonable care to ensure that the mechanism of notification and the period of notification do not prejudice participants in the PKI and are in the best interests of the proper and secure operation of the PKI.

9.12.3 Circumstances under which OID must be changed

The Policy Authority determines whether CPS changes require and amendments.

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.

9.14 Governing Law

The entire provisions of this LAWtrust AeSign Certificate Authority 2048 CPS and any Subscriber's Agreement or Relying Party Agreement entered into pursuant to this LAWtrust AeSign Certificate Authority 2048 CPS shall be governed by and construed in accordance with the laws of the Republic of South Africa as it pertains to its applicability and usage inside the Republic of South Africa. Furthermore, the parties hereto irrevocably and unconditionally

consent to the non-exclusive jurisdiction of the relevant court in the Republic of South Africa, as the case may be, in regard to the enforcement of any rights relating to all matters arising from this LAWtrust AeSign Certificate Authority 2048 CPS.

Where the digital certificate issued in terms of this CPS and Subscriber Agreement is issued to a party that is a citizen or resident of a country other than South Africa, then this document will be subject to the provisions of the jurisdiction of South Africa. In the event of a dispute between LAWtrust and a digital certificate user, who is a citizen or resident of a country outside the Republic of South Africa, such dispute will be dealt with in accordance with the Rules of the London Court for Arbitration.

9.15 Compliance with Applicable Law

This CPS is subject is subject to all applicable laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The provisions of the LAWtrust AeSign Certificate Authority 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 AeSign Certificate Authority 2048 CPS and those agreements. No representations (save for any fraudulent misrepresentations) terms, conditions or warranties not contained in the LAWtrust AeSign Certificate Authority 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 AeSign Certification Authority 2048 CPS, without the prior written consent of the LAWtrust PA.

9.16.3 Severability

To the extent that any provisions of the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 CPS or Relying Party Agreements and all other provisions of the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 2048 will be treated according to the laws of the Republic of 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 AeSign Certification Authority 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 Merger

Nothing contained in this CPS shall be deemed to constitute either the LAWtrust AeSign Certification Authority 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 AeSign Certification Authority 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 AeSign Certification Authority 2048.

10. 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

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

Term	Definition
	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 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:

Term	Definition
	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.

Term	Definition
hosted data centre	The LAWtrust hosted data centre is the facility at Vodacom.
Identity document	An identity document is used to verify aspects of a person's identity. Recognised identity documents are; For South African citizens, 1. a valid "Green" Identity document or Passport issued by the South African Home Affairs department 2. A valid South African Driver's license For non-South African Nationals, 1. a valid Passport issued by the persons country of origin Home Affairs department.
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)

Term	Definition
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.
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.

Term	Definition
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
SCD	Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature
Secure Key Store	Technology component (Software of Hardware) which enables a mechanism to generate, store and use cryptographic keys in a secure manner.

Term	Definition
Secure Signature-Creation Device (SSCD)	A secure personalised device with cryptographic capabilities in which a subscriber electronic signature creation data (SCD) will be generated and all encryption operations are performed in the SSCD. SCD generation and use is with sole control of the subscriber.
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.
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.

11. SIGN OFF ACCEPTANCE

Name:	Marcile De Waal
Authority:	Policy Authority
Title:	Senior Specialist: Cryptographic Services
Date:	2026-10-16
Signature:	