	<b>INFORMATION SECURITY POLICY</b>
	<b>ISSUE SPECIFIC POLICY</b>
	<b>VERSION: VI05 2018-12-12</b>
	<b>EFFECTIVE DATE: 2018-12-12</b>

# LAWtrust AeSign CA Certification Practice Statement (LAWtrust AeSign CPS)

---

## Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07


("LAWtrust")

85 Regency Drive,  
Route 21 Corporate Park, Irene, Centurion,  
Pretoria, South Africa

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

Web <https://www.lawtrust.co.za> • eMail [governance@lawtrust.co.za](mailto: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.*


 <b>Lawtrust</b>   an <b>ETION</b> <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

**COPYRIGHT NOTICE**

**LAW TRUSTED THIRD PARTY (PTY) LTD (“LAWTRUST”) RETAINS THE COPYRIGHT IN THIS CERTIFICATION PRACTICE STATEMENT (“CPS”) AS WELL AS ANY NEW VERSIONS OF IT PUBLISHED AT ANY TIME BY LAWTRUST.**

**LAWTRUST FURTHER RETAINS THE COPYRIGHT IN ALL DOCUMENTS PUBLISHED OR APPROVED BY THE LAWTRUST POLICY AUTHORITY (“LAWTRUST PA”) UNDER AND IN TERMS OF THE PROVISIONS OF THIS LAWTRUST CPS.**


**THE COPYING OR DISTRIBUTION OF THIS CPS OR DOCUMENTS APPROVED BY THE LAWTRUST PA, IN WHOLE OR IN PART, AND CONTRARY TO THE PROVISIONS OF THIS CPS WITHOUT THE PRIOR WRITTEN CONSENT OF THE LAWTRUST PA, IS STRICTLY PROHIBITED.**

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 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
V004 2017-10-19 V003 2017 05 11	2017-02-27	Bruce Anderson	Included various housekeeping items. Included the use of SSCD	Expired
V003 2017-05-11	2017-05-11	Bruce Anderson	Corrected invalid links	Expired
V004 2017-10-19	2017-10-19	Bruce Anderson	2017 review	Expired
VI05 2018-12-12	2018-12-12	Eduard Oosthuizen	QA Review, apply new document template, 2018 Review	Operational

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## Document references


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

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

 <b>Lawtrust</b> an <b>ETION</b> <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>11</b>
1.1	Overview.....	11
1.2	Document name and identification .....	12
1.3	PKI participants.....	12
1.4	Certificate usage .....	14
1.5	Policy administration.....	15
1.6	Definitions and acronyms .....	19
<b>2.</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>32</b>
2.1	Repositories.....	32
2.2	Publication of certification information .....	33
2.3	Time or frequency of CPS publication .....	34
2.4	Access controls on repositories .....	34
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION.....</b>	<b>35</b>
3.1	Naming .....	35
3.2	Initial identity validation .....	37
3.3	Identification and authentication for re-key requests .....	39
3.4	Identification and authentication for revocation request .....	40
<b>4.</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>42</b>

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

4.1 Notification mechanism .....43

4.2 Certificate application.....43

4.3 Certificate application processing .....44

4.4 Certificate issuance.....46

4.5 Certificate acceptance .....47

4.6 Key pair and certificate usage .....47

4.7 Certificate Renewal .....49

4.8 Certificate re-key .....50

4.9 Certificate modification.....52

4.10 Certificate revocation and suspension.....53

4.11 Certificate status services .....62

4.12 End of Subscription.....63

4.13 Key escrow and recovery policy and practices .....63

**5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS .....63**

5.1 Physical controls.....63


5.2 Procedural controls .....65

5.3 Personnel controls .....68

5.4 Audit logging procedures .....71

5.5 Records archival.....71

5.6 Key changeover .....72

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

5.7 Compromise and disaster recovery .....73

5.8 LAWtrust AeSign CA or LAWtrust AeSign RA termination .....74

5.9 LAWtrust AeSign CA impact on third party functionality .....74

5.10 Escalation of physical security violations .....74

**6. TECHNICAL SECURITY CONTROLS .....74**

6.1 Key pair generation and installation .....74

6.2 Private key protection and cryptographic module engineering controls .....76

6.3 Other key management aspects .....77

6.4 Activation data .....79

6.5 Computer security controls .....79

6.6 Life cycle technical controls .....80

6.7 Network security controls .....80

6.8 Time-stamping .....81

6.9 Information security .....81

6.10 Escalation of information security violations .....81

6.11 Secure communication between the RA and the CA .....81


6.12 Security Management .....81

**7. CERTIFICATE PROFILES .....82**

7.1 Certificate profile .....82

7.2 CRL profile .....86



 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

7.3 OCSF profile .....86

**8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....87**

8.1 Frequency or circumstances of assessment .....87

8.2 Identity/qualifications of assessor .....87

8.3 Assessor's relationship to assessed Entity .....87

8.4 Topics covered by assessment.....87

8.5 Actions taken as a result of deficiency .....88

8.6 Communication of results .....88

**9. OTHER BUSINESS AND LEGAL MATTERS .....88**

9.1 Fees .....88

9.2 Financial responsibility .....89

9.3 Confidentiality of business information .....90

9.4 Privacy of personal information .....92

9.5 Intellectual property rights .....93

9.6 Representations and warranties.....94


9.7 Disclaimers of warranties.....97

9.8 Limitation of liability .....98

9.9 Indemnities .....98

9.10 Term and termination .....98

9.11 Individual notices and communications with participants.....99

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

9.12 Amendments .....99

9.13 Dispute resolution.....100


9.14 Governing law .....100

9.15 Compliance with applicable law.....101

9.16 Miscellaneous provisions .....101

9.17 Other provisions .....102

**10. SIGN OFF ACCEPTANCE.....103**

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

# 1. INTRODUCTION

## 1.1 Overview


LAWtrust is an accredited Authentication Service Provider by the South African Accreditation Authority (SAAA) in terms of the Electronic Communications and Transactions Act 2002 for the provision of Advanced Electronic Signatures.

AeSign is the LAWtrust trademark for Advanced Electronic Signature products and services. This document is the LAWtrust Advanced Electronic Signature Certification Practice Statement (LAWtrust AeSign CPS) for the LAWtrust AeSign CA.

This LAWtrust AeSign CPS describes the certification practices that have been implemented to ensure the LAWtrust AeSign CA trustworthiness in issuing public key certificates to Subscribers. The certificates will reside on a secure signature creation device (SSCD) personalised to the subscriber and the subscriber unique electronic signature creation data will be generated and used on the SSCD. The LAWtrust AeSign CPS has been drafted to satisfy the requirements of the LAWtrust AeSign CA for issuing LAWtrust AeSign Certificates.

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

This LAWtrust AeSign CPS also prescribes the practices and procedures which the LAWtrust AeSign CA will require of all Registration Authorities (LAWtrust AeSign RA's) operating under its authority as well as the rights and obligations of third parties including, but not limited to, Applicants, Subscribers and Relying Parties.

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 1.2 Document name and identification

This document title is "LAWtrust AeSign CA Certification Practice Statement (LAWtrust AeSign CA CPS)" The document name is LT\_ISP\_AES\_CPS. You may consider the version of the LAWtrust AeSign CPS available for download from the LAWtrust website [<https://www.lawtrust.co.za/repository>] as the most current and authoritative version as at the time of downloading.

## 1.3 PKI participants

### 1.3.1 LAWtrust AeSign CA

The LAWtrust AeSign CA is chained into the public hierarchy of the LAWtrust Root Certificate Authority. This offers certificates with the following hierarchies

LAWtrust Root Certification Authority

↳ LAWtrust AeSign CA Certification Authority

↳ Subscriber


The LAWtrust AeSign CA may:

- Accept the certificate signing requests ("CSR") with the public keys of an Applicant from a LAWtrust AeSign RA which has authenticated the identity and verified information to be contained in the LAWtrust AeSign CA Certificate applied for by the Applicant;
- Once the CSR is verified the LAWtrust AeSign CA will create a LAWtrust AeSign CA Certificate containing the signed public key.

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

### 1.3.2 Registration authorities

The LAWtrust AeSign CA may authorise representatives or agents, including LAWtrust AeSign RA's (as agreed in a Managed PKI Services Agreement (MSA) and related Supplementary Agreements with the RA) to:

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

- Accept applications for a LAWtrust AeSign Certificate;
- Perform authentication of identities and verification of information submitted by Applicants when applying for a LAWtrust AeSign CA Certificate in terms of the appropriate LAWtrust Registration Authority Charter approved by the LAWtrust Policy Authority (LAWtrust PA); where such authentication and verification is successful, submit the CSR to the LAWtrust AeSign CA, in accordance with the provisions of this LAWtrust AeSign CPS
- Secure the part of the certificate lifecycle processes for which the LAWtrust AeSign RA assumes responsibility as stated in the MSA and LAWtrust AeSign RA Charter, excluding the automated RA services provided by the LAWtrust AeSign RA software and the LAWtrust AeSign CA.

### 1.3.3 Applicants

An Applicant is a person, Entity, or organisation that has applied for but has not yet been issued a LAWtrust AeSign CA Certificate.

### 1.3.4 Subscribers


A Subscriber is a person, Entity, or organisation that has been issued a LAWtrust AeSign CA Certificate. A subscriber will be issued with a Secure Signature Creation Device (SSCD) on which the electronic signature creation data (SCD) will be generated and used under the subscriber's sole control. The SCD will include the digital certificate private key.

#### 1.3.4.1 Structure of the SSCD

The subscriber will have complete control of the SSCD and the use of the SSCD will be exclusive to the subscriber.

Subscriber

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

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

### **1.3.5 Relying parties**

A Relying Party is a person, Entity, or organisation that relies on or uses a LAWtrust AeSign CA Certificate and/or any other information provided in the LAWtrust repository to verify the identity and public key of a Subscriber and/or use such public key to send or receive encrypted communications to or from a Subscriber.

### **1.3.6 Other participants**

Other participants are Entities or organisations within South Africa on whom LAWtrust will rely in verifying information relating to an Applicant for issuing a LAWtrust AeSign CA Certificate.

## **1.4 Certificate usage**

The LAWtrust AeSign CA is capable of manufacturing two certificate types; managed or enterprise certificates and unmanaged or web certificates. The significant difference between the two is that key recovery is available for managed certificates. The functionality of signing and encryption is the same for both certificates. The specifics of the certificate to be used will be defined in a Registration Authority Charter workshop.

### **1.4.1 Prohibited certificate uses**


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

Any use falling outside the LAWtrust AeSign Certificate uses described in this AeSign CPS will be deemed a prohibited use.

### **1.4.2 Appropriate certificate uses**

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

- To digitally sign electronic documents and transactions.

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 1.5 Policy administration

### 1.5.1 Security Management

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

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).

### 1.5.2 Roles and responsibilities

In order to ensure universal adoption of the Policies, LAWtrust has set up a Security Committee and two authority bodies comprising of senior management membership.

The Security Committee is appointed to support a structured management framework which directs, monitors and controls the implementation of information security as a whole within LAWtrust.


The LAWtrust Policy Authority (LAWtrust PA) will be responsible for all Policy administration; such policies include documents listed in section 1.5.1.

The LAWtrust Operating Authority (LAWtrust OA) is the body responsible for the LAWtrust AeSign CPS operational implementation, this includes all procedures and standards required to ensure correct implementation of the LAWtrust AeSign CPS.

The LAWtrust AeSign CPS is based on the policies established by the LAWtrust PA.

### 1.5.3 Organisation administering the document

The LAWtrust Policy Authority, (LAWtrust PA) will administer all the policies and practices relating to the LAWtrust Certificate Authorities; this includes the LAWtrust CP, CPS and

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

RA's. The LAWtrust Operations Authority (LAWtrust OA) will be responsible for the implementation of the LAWtrust AeSign CPS and related procedures.

#### **1.5.4 Policy change procedures**

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

##### **1.5.4.1 Process for CPS change requests**

1. Requests are submitted to the PA via email at the email address stipulated in section 1.5.2.
2. The PA will
  - a. review proposed changes to the CPS,
  - b. analysis of the impact of the changes together with the OA.
  - c. Make recommendations to the LAWtrust SC for approval.
3. On SC approval, the PA will sign off the changed document and the proposed changes will be planned and implemented taking into account notification procedures as described in sections 1.5.4.2 and 1.5.4.3 below.


##### **1.5.4.2 Low impact modifications**

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

##### **1.5.4.3 High Impact modifications**

Modifications to the LAWtrust AeSign CPS that, in the judgment of the LAWtrust PA may have a significant impact on Applicants, Subscribers, and Relying Parties, will be



 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

published in the LAWtrust Repository and will become effective thirty (30) days after notification of such changes.

#### 1.5.4.3.1 Definition of significant impact modifications

Modifications which are considered to have high impact include the following:

1. Changes to the subscriber identification process
2. Changes to the reliance limit of the certificates
3. Changes in encryption key generation, storage or usage

#### 1.5.4.3.2 Version Control

In the event that the LAWtrust PA makes significant modifications to LAWtrust AeSign CPS, the version number of the LAWtrust AeSign CPS will be updated accordingly.

#### **1.5.4.4 Subscriber acceptance of CPS Changes**


Unless a Subscriber ceases to use, removes, and requests revocation of such Subscriber’s LAWtrust AeSign CA Certificate(s) prior to the date on which an updated version of the LAWtrust AeSign CPS becomes effective, such Subscriber will be deemed to have consented to the terms and conditions of such updated version of the LAWtrust AeSign CPS and will be bound by the terms and conditions of such updated version of the LAWtrust AeSign CPS.

#### **1.5.5 Person determining CPS suitability for the policy**

The LAWtrust PA will determine suitability of the LAWtrust AeSign CPS for the LAWtrust AeSign CA Certificate Policy.

#### **1.5.6 Publication and notification policies**

Prior to any significant changes to this LAWtrust AeSign CPS being published, as described in 1.5.4, LAWtrust will provide the following notification with 30 days prior to publication

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

### **1.5.7 CPS approval procedures**

The LAWtrust AeSign CPS is developed by the LAWtrust PA and the LAWtrust OA and approved by the LAWtrust PA.

### **1.5.8 Contact Detail**

The contact information for questions to the LAWtrust PA and LAWtrust OA is:


85 Regency Drive,  
Route 21 Corporate Park, Irene,  
Centurion,  
South Africa

Phone +27 (0)12 676 9240

Fax +27 (0)12 665 3997


<https://www.lawtrust.co.za>

eMail: [governance@lawtrust.co.za](mailto:governance@lawtrust.co.za) (PA) or [mpkiops@lawtrust.co.za](mailto:mpkiops@lawtrust.co.za) (OA)


 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 1.6 Definitions and acronyms


<b>Term</b>	<b>Definition</b>
applicant	A person, Entity or organisation 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	<p>A factor of authentication refers to a mechanism used to facilitate the authentication of a user or devices requesting access to computing resources.</p> <p>The following factors of authentication are universally accepted;</p> <p>Location of the computing interface(controlled access and managed),</p> <p>Something the requester has(Possession of something which is validated),</p> <p>Something the requester knows(secret password or PIN),</p>

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
	Something the requester is(biometrics)
Authentication scheme	Industry accepted authentication schemes include one or more factors of authentication. The choice of authentication factors and the process behind establishing credentials within each factors within the chosen scheme determine the strength of the authentication.
CA	See definition of certificate/certification authority.
certificate administrator	A trusted individual that performs certain trusted tasks (e.g. authentication) on behalf of a CA or RA. This person is usually a member of the personnel of such CA or RA.
Certificate	See definition of digital certificate.
certificate/certification authority	A 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.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
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.
Client SSCD	<p>Client SSCD is one which is issued to a subscriber and the SSCD is maintained by the subscriber.</p> <p>The client SSCD will have the subscriber electronic signature data (SCD) generated on the SSCD and all encryption operations are performed on the SSCD. SCD generation and use is within sole control of the subscriber.</p>
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 subordinate CA's and or Issuing CA's.

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

<b>Term</b>	<b>Definition</b>
cryptography	Cryptography is about message secrecy, and is a main component in information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, not usually the existence of such messages.
cryptography services	A service provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of a digital certificate/digital signature scheme for the purpose of ensuring (i) that data or data messages can be accessed or can be put into an intelligible form only by certain persons, (ii) that the authenticity or integrity of such data or data message is capable of being ascertained, (iii) the integrity of the data or data message, or (iv) that the source of the data or data message can be correctly ascertained.
Data	Electronic representations of information in any form.
data message	Data generated, sent, received or stored by electronic means.
digital certificate	A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number.


 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

<b>Term</b>	<b>Definition</b>
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: <ol style="list-style-type: none"> <li>1. decrypting the signature object with the public key component to expose the original hash value,</li> <li>2. re-computing a hash value over the data object, and</li> <li>3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.</li> </ol>
digitally sign	The act of generating a digital signature for a data message, which is created by: <ol style="list-style-type: none"> <li>1. Hashing the object to be signed with a one-way hash function; and</li> <li>2. Encrypting (signing) the hash value with the private key component of a key pair.</li> </ol> <p>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</p>


 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

<b>Term</b>	<b>Definition</b>
	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.
electronic signature creation data or SCD	“electronic signature creation data” means unique data which is used by the signatory to create an electronic signature




 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
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.
Identity Documents for a company, close corporation or other legal entity	<p>Where the subscriber is a company, close corporation or other legal entity</p> <ol style="list-style-type: none"> <li>1. the relevant constitutive documents,</li> <li>2. resolution or power of attorney of the directors, authorising a specific person to apply for or otherwise deal with LAWtrust in relation to the issuing, renewal or replacement of certificates; and</li> </ol> <p>the identity documents applicable for natural persons for each of the directors, members of trustees of the applicant and the authorised key holder together with a resolution appointing the representative as the authorise key holder.</p>
Identity documents for Natural persons	<p>Where the subscriber is a natural person, the following documents must be used for the authentication and verification of a subscriber, during initial registration, certificate renewal, routine rekey, rekey after revocation and when processing requests for suspension or revocation,</p> <ol style="list-style-type: none"> <li>1. Identity document or Passport for initial registration</li> <li>3. Accredited certificate for Certificate renewal</li> </ol>
Identity documents for partnerships	<p>Where the subscriber is a partnership,</p> <ol style="list-style-type: none"> <li>1. the constitutive documents of the partnership, if applicable and</li> <li>2. the identity documents applicable for natural persons.</li> </ol>

 <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
Identity document	<p>An identity document is used to verify aspects of a person's identity. Recognised identity documents for natural persons are;</p> <p>For South African citizens,</p> <ol style="list-style-type: none"> <li>1. A valid and original "Green" Identity document or National ID Card issued by the South African Department of Home Affairs</li> <li>2. A valid and original Passport issued by the South African Department of Home Affairs</li> <li>3. A valid and original temporary identity document issued by the South African Department of Home Affairs</li> </ol> <p>For non-South African Nationals,</p> <ol style="list-style-type: none"> <li>1. a valid and original Passport issued by the applicant or subscribers country of origin Home Affairs department.</li> </ol>
Integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
Key Encryption Key or KEK	A Key Encryption Key (KEK) is a cryptographic key that is used for encrypting other cryptographic keys.
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).
Key Wrapping	Key wrapping is a cryptographic construct that uses symmetric encryption to encapsulate key material.
LAWtrust Root CA	See also the definition of certification authority. The Root certification authorities managed by LAWtrust including the LAWtrust Root

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
	Certification Authority 2048 and the LAWtrust Root Certification Authority 2 (4096)
LAWtrust Subordinate CA Certificate	See definition of digital certificate. All digital certificates issued by a LAWtrust Subordinate.
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.
LDAP	A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Master Services Agreement	The contract between LAWtrust and an appointed registration authority stipulating the terms and conditions for the registration authority to manage certificate lifecycle activities on behalf of the LAWtrust Root CA.
MSA	Master Services Agreement,
non-repudiation	The ability to prevent a party from refusing to fulfil an obligation or denying the truth or validity of an electronic communication facilitated by appropriate use of the LAWtrust Services.

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
OCSP	Online Certificate Status Protocol is an Internet protocol, employed to ascertain the revocation status of an X.509 digital certificate. An alternative to CRL based checking.
OCSP Responder	An online service hosted by LAWtrust and connected to LAWtrust repositories in order to process OCSP certificate revocation checks.
private key	The key of a key pair used to create a digital signature and is required to be kept secret.
public key	The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed.
Public key cryptography	Public key cryptography is about using mathematically related keys, a public key and a private key, in order to implement a digital certificate /digital signature scheme, also known as an asymmetric crypto system.
PKI	See definition of public key infrastructure.
public key infrastructure	The structure of hardware, software, people, processes and policies that collectively support the implementation and operation of a certificate-based public key cryptography scheme.

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>


<b>Term</b>	<b>Definition</b>
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
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.
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

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

<b>Term</b>	<b>Definition</b>
	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.
subscriber agreement	An agreement between the certificate authority and a subscriber that sets out the terms and conditions governing the issuance of a certificate, control of the private key that corresponds to the public key listed in the certificate, acceptable use of the certificate, notification of compromise of the private key, and matters ancillary and related thereto.
System	A System is a collection of components (HW, SW, DB, process) organised in a manner to provide specific outcomes.
Trustworthy System	<p>A trustworthy system is</p> <ol style="list-style-type: none"> <li>1. A system which is protected against modification and ensures the technical security and reliability of the processes supported by them;</li> <li>2. Can be used to store data provided to it, in a verifiable form so that: <ul style="list-style-type: none"> <li>(i) the systems are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,</li> </ul> </li> </ol>

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

<b>Term</b>	<b>Definition</b>
	<p>(ii) only authorised persons can make entries and changes to the stored data,</p> <p>(iii) the data can be checked for authenticity;</p>
Verification	<p>Verification is the act of checking that information is accurate. It is used in the following manor</p> <p>a) At registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity;</p> <p>b) During use, the act of comparing electronically submitted identity and credentials with stored values to prove identity.</p> <p>c) Relying Party will check the certificates used as per the relying Party Agreement.</p>

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 Repositories

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

#### 2.1.1 Document repository

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


- The LAWtrust AeSign CPS,
- The LAWtrust AeSign RA Charter's (where RA approval was obtained for publication),
- Information and agreements relating to the subscription for and reliance on LAWtrust AeSign CA Certificates;
- LAWtrust AeSign CA public certificates;
- 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 this LAWtrust AeSign CPS.

#### 2.1.2 Certificate status repository

The certificate status checking is available via certificate revocation lists and OCSP for external use and LDAP for internal use.



 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 2.1.3 External access

CRL 1(web interface access):

The LAWtrust AeSign CA Certificate Revocation List (CRL) are accessible through the web-interface

[\[http://aesigncrl.lawtrust.co.za/CRL/lawtrust\\_aesign\\_ca\\_crlfile.crl\]](http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl) and is periodically updated in terms of this LAWtrust AeSign CPS.

Online Certificate Status Protocol

OCSP Responses are available 24 hours a day, 7 days a week as described in section 4.10.12.

### 2.1.4 Internal access

CRL 2 (light-weight directory access protocol (LDAP) access):

The LAWtrust AeSign CA Certificate Revocation List (CRL) are also published to the LDAP interface:

*[ldap://ldap.hostname:389/cn=LAWtrust AeSign Certification Authority 2048,ou=LAW Trusted Third Party,Services PTY Ltd,o=LAWtrust,c=ZA]*


and is periodically updated in terms of this LAWtrust AeSign CPS.

## 2.2 Publication of certification information

### 2.2.1 Publication of the LAWtrust AeSign CPS

This LAWtrust AeSign CPS, published in the LAWtrust repository, will 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 CPS will be published in accordance with directions given by the LAWtrust PA.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 2.2.2 Publication and notification policies

Prior to any significant changes to this LAWtrust AeSign CPS being published, as described in section 1.5.

LAWtrust shall provide the following notification with 30 days prior to publication

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

### 2.3 Time or frequency of CPS publication

After acceptance by the LAWtrust PA this LAWtrust AeSign CPS will be published in the manner described in section 2.2.


This LAWtrust AeSign CPS will 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 CA provide certificates.
- Annual Review of the LAWtrust AeSign CPS

Changes will be documented in revised versions of this LAWtrust AeSign CPS and become effective on the dates indicated in the revised CPS.

### 2.4 Access controls on repositories

This LAWtrust AeSign CPS and all other documents published in the LAWtrust Repository will be available to all Applicants, Subscribers and Relying Parties, but may only be modified by the LAWtrust PA. The LAWtrust PA will digitally sign LAWtrust AeSign CA related documents published in the repository to protect the document integrity.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 3. IDENTIFICATION AND AUTHENTICATION

Before issuing a certificate a LAWtrust AeSign RA will authenticate the identity and/or attributes of an Applicant to be published in a LAWtrust AeSign CA Certificate. This section of the LAWtrust AeSign CPS establishes the criteria for an acceptable application for a LAWtrust AeSign CA Certificate and for the authentication of persons requesting the revocation of a LAWtrust AeSign CA Certificate.

#### 3.1 Naming

##### 3.1.1 Types of names

A LAWtrust AeSign CA Certificate will include a common name component as required in the X.501 Standard. The common name will 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 (or preferred name entered on the application form), 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.

##### 3.1.3 Anonymity or pseudonymity of Subscribers

LAWtrust will only provide anonymous certificates or certificates to individuals under a pseudonym for dedicated Certificate Authority roles. In cases where the LAWtrust AeSign

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

CA 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.

### **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.


### **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 will not re-use a serial number in respect of a LAWtrust AeSign CA Certificate.

### **3.1.6 Name claim dispute resolution**

The common names in LAWtrust AeSign CA Certificates are issued on a “first come, first served” basis. By accepting a common name for incorporation into a LAWtrust AeSign CA Certificate, an RA operating under a LAWtrust AeSign CA 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, legal Entity, or organization. The LAWtrust AeSign CA and any RA’s operating under the LAWtrust AeSign CA 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 CA Certificate.

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### **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 9.13 of this CPS

## **3.2 Initial identity validation**

The LAWtrust AeSign RA 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 RA Charter of the LAWtrust AeSign RA 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 relevant Registration Authority Charter (LAWtrust AeSign RA Charter) of a LAWtrust AeSign RA. This requires an Applicant to generate a CSR signed with its private key and the LAWtrust AeSign CA validating the signature with the Applicant's public key.


In all instances in which the LAWtrust AeSign RA Charter of a LAWtrust AeSign RA 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**

#### **3.2.2.1 Authentication of Entity registered on CIPC or accredited database**

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,

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

2. the relevant constitutive documents,
3. resolution or power of attorney of the directors, authorising a specific person to apply for or otherwise deal with LAWtrust in relation to the issuing, renewal or replacement of certificates; and
4. the identity documents applicable for natural persons for each of the directors, members of trustees of the applicant and the authorised key holder together with a resolution appointing the representative as the authorise key holder.

### **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 or Passport for initial registration
2. Accredited certificate for Certificate renewal

#### **3.2.3.2 Authentication of a personal identity eMail address**

In cases where the LAWtrust AeSign CA Certificate will be used for digitally signing and/or encrypting eMail the LAWtrust AeSign RA 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 CA Certificate.

### **3.2.4 Non-verified Subscriber information**

Certain information gathered for the purpose of certification may not be verified by a LAWtrust AeSign RA. All the information published in a LAWtrust AeSign CA Certificate will be verified by LAWtrust AeSign RA as stipulated by the LAWtrust PA.

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 3.2.5 Validation of authority

The LAWtrust AeSign CA is the authority to which any RA's under the LAWtrust AeSign CA have been created. As such all rights, entitlements or permissions of Subscribers within a specific organisation RA will be specified within the specific organisation LAWtrust AeSign 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 LAWtrust AeSign RA will 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 CA Certificate subject to a routine re-key in the manner determined in a LAWtrust AeSign RA Charter. The stringency of authentication of identity and verification of information will 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 CA will not renew or re-issue LAWtrust AeSign CA Certificates that have been permanently revoked.

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

A Subscriber will be required to complete a new application process as and authenticate as described in 3.2 including generation of a new key-pair and submission of all information required for an initial application for a LAWtrust AeSign CA Certificate as stipulated in the LAWtrust AeSign RA Charters.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

On revocation of a LAWtrust AeSign CA Certificate the Subscriber will immediately cease using such a LAWtrust AeSign CA Certificate and remove the LAWtrust AeSign CA Certificate from any devices and/or software in which it has been installed.

### **3.4 Identification and authentication for revocation request**

A LAWtrust AeSign RA will 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 a LAWtrust AeSign RA Charter, which will be approved by the LAWtrust PA. See section 3.2 for authentication requirements,

#### **3.4.1 Access and permissions to revoke**

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

1. The LAWtrust AeSign RA must nominate RA personnel to be the certificate administrators.
2. The nominated RA personnel must fill in and sign application forms
3. The application form must be collected in person by the 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 CA. The permissions will be restricted to the specific LAWtrust AeSign RA concerned.

#### **3.4.2 Revocation Request format**

Revocation requests may be sent to the RA email address as specified in the relevant RA Charter.

1. The format of the email should include the following
2. Requester name, designation and organisation
3. Reason for and severity of the revocation request
  - a. Severity 1: suspected key and or password compromise,



 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

- b. Severity 2: lost, stolen or corrupted key store,
  - c. Severity 3: Business related reason (end of business relationship or change in permissions) or other valid reasons.
4. Provide details of the events leading up to the point of defining a reason
  5. Date and time of any events, relating to the reason for the revocation request.
  6. The email 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 with 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,

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

2. CRL update within 8 hours of revocation 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 within 24 hours of revocation 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 within 24 hours of revocation performed.
3. OCSP update cycle, 30 minutes

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

LAWtrust appoints the LAWtrust AeSign RA's to perform the certificate lifecycle operations and management according to the processes specified in the LAWtrust AeSign RA Charters. The process of RA authorisation and appointment will be set out in a MSA between LAWtrust and the specific RA as stipulated in the SAAA Accreditation Regulations on the delegation of certificate lifecycle functions to agents. All RA responsibilities relating to the processes and security must be contained in the LAWtrust AeSign RA Charter.

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### 4.1 Notification mechanism

Certificate lifecycle notification between the 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 (or any additional role specified in a LAWtrust AeSign RA Charter) may submit a certificate application to the approved LAWtrust AeSign RA Certificate Administrator.

The LAWtrust AeSign CA will, under this LAWtrust AeSign CPS, issue:

1. LAWtrust AeSign CA Certificates in respect of natural persons.
2. LAWtrust AeSign CA 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 RA an application for a LAWtrust AeSign CA 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 CPS and the applicable Subscriber Agreement;
3. Make payment to the LAWtrust AeSign CA and/or LAWtrust AeSign RA of all fees and charges in respect of the application for the issue of the LAWtrust AeSign CA Certificate.

###### 4.2.2.2 Registration Authority

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

 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

If the application or information provided to the LAWtrust AeSign RA is deficient, the LAWtrust AeSign RA shall, at its discretion:

1. Use commercially reasonable efforts to notify the applicant by eMail at the eMail address provided for in the application, or in person, of the deficiency and of the refusal of the application.

If the verification of the information submitted to the LAWtrust AeSign 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 CA Certificate onto the SSCD which has been issued to them.

After the issue of the LAWtrust AeSign CA Certificate neither the LAWtrust AeSign CA nor any LAWtrust AeSign 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 CA Charter.

### **4.3 Certificate application processing**

#### **4.3.1 Performing identification and authentication functions**

The LAWtrust AeSign CA will process an application for the issue of a LAWtrust AeSign CA Certificate only after a LAWtrust AeSign RA has performed the authentication and verification checks provided for in the relevant LAWtrust AeSign RA Charter.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **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. Use a best effort to verify the applicants email address.

Once the authentication and verification process has been completed the LAWtrust AeSign RA will 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.

#### **4.3.1.2 Generating and issuing relevant codes**


On successful verification and authentication of the subscriber, the administrator will authenticate to the RA interface and use the RA interface, to issue the authentication code and reference number.

These codes will be shared with the applicant in an out of band mechanism.

In the case of an automated RA service, any codes are issued by the CA and consumed by the RA automated service to issue the digital certificate.

#### **4.3.2 Approval or rejection of certificate applications**

Approval of a certificate application will result in the process continuing. Application rejection will result in notification by the relevant RA to the Applicant of the reason for the rejection, as set out in section 4.2.2.

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### **4.3.3 Time to process certificate applications**

Any application for a certificate should be processed within the time stipulated in the specific LAWtrust AeSign RA Charter. The LAWtrust AeSign CA will process a CSR immediately on receiving such a request.

### **4.3.4 Time to publish certificates in the certificate directory**

The LAWtrust AeSign CA 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 CA can only accept certificate issuance requests from authorised LAWtrust AeSign RA instances. These RA components are authenticated using a LAWtrust AeSign CA profile certificate and a secure certificate management protocol between the LAWtrust AeSign RA component and the LAWtrust AeSign CA. After satisfying itself that the information provided to it by a LAWtrust AeSign RA is accurate and that the authentication and verification checks required by the LAWtrust PA have been executed, the LAWtrust AeSign CA may generate and digitally sign the LAWtrust AeSign CA Certificate applied for in accordance with the certificate profile described in 7.1 of this LAWtrust AeSign CPS.

### **4.4.2 Notification to Subscriber by the RA of issuance of certificate**

On successful issuance of the certificate, the LAWtrust appointed AeSign RA agent (or agent software) will make reasonable efforts to notify the subscriber which may include in person verbal communication or sending an eMail to the Subscriber (at the eMail address provided in the certificate application), stating that the certificate has issued.

The certificate will be immediately delivered to the client SSCD and issued to the Subscriber.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 4.5 Certificate acceptance

### 4.5.1 Conduct constituting certificate acceptance

After issuance of the LAWtrust AeSign CA Certificate and notification addressed to the Subscriber, the Subscriber will check that the content of the LAWtrust AeSign CA Certificate is correct.

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

By using the LAWtrust AeSign CA Certificate in any manner contemplated in this LAWtrust AeSign CPS, the Subscriber accepts the accuracy of the information contained in the LAWtrust AeSign CA Certificate.

If the appropriate LAWtrust AeSign RA is notified of any inaccuracies in the LAWtrust AeSign CA Certificate by the Subscriber the LAWtrust AeSign CA Certificate will be revoked in terms of the provisions of 4.10 of this LAWtrust AeSign CPS.

### 4.5.2 Publication of the certificate by the CA

Post issuance the certificate is published in the LAWtrust AeSign CA directory for internal CA processing.


### 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 CA Certificate.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

The Subscriber shall use his/her private key and the LAWtrust AeSign CA Certificate in strict compliance with the Subscriber Agreement entered between the Subscriber and LAWtrust and this LAWtrust AeSign 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 MSA's between LAWtrust and all RA's.

#### **4.6.2 Relying Party public key and certificate usage**

Relying Parties will comply strictly with the provisions of the Relying Party Agreement entered into between the Relying Party and LAWtrust and will be responsible for checking the status of any LAWtrust AeSign CA Certificate before relying on the certificate.

#### **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 can be stored on a client SSCD.

No Client supplied client SSCD's will be allowed without approval from the Policy Authority in writing.


#### **4.6.4 Life cycle management of the SSCD.**

##### **4.6.4.1 Client SSCD**

The client SSCD lifecycle can be described as follows

1. SSCDs are ordered from the supplier
2. SSCDs are pre-initialised with the LAWtrust configuration
3. Pre-initialised SSCDs are provided to enrolment officers to issue to subscribers.



 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

4. SSCDs are issued to subscribers, at the same time that the digital certificate requirement for face-to-face identity verification is performed.
5. SSCDs and the digital certificate which resides on the SSCD are used by the subscriber
6. If a SSCD is lost or stolen or compromised, the certificate is revoked and new SSCD and certificate is issued.
7. 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**

LAWtrust AeSign CA Certificates may be renewed provided that the LAWtrust AeSign RA conducts and confirms that it has conducted the necessary authentication and verification checks for the purposes of the certificate renewal in accordance with the LAWtrust AeSign RA Charter approved by the LAWtrust PA.

##### **4.7.1 Circumstance for certificate renewal**


LAWtrust AeSign CA Certificates should be renewed under the following circumstances

1. All LAWtrust AeSign CA certificates should be renewed prior to the certificate "valid until" date.
2. The subscriber agrees to the autorenewal of the certificate.
3. The CA will perform the following checks prior to renewal.
  - a. Is the certificate an accredited certificate
  - b. Is the certificate valid

##### **4.7.2 Who may request renewal**

LAWtrust AeSign CA certificate renewal can be requested by the following

1. The LAWtrust AeSign CA Subscriber

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

2. An approved LAWtrust AeSign CA RA

In the case of autorenewal, the subscriber agrees to the auto-renewal of the certificate, the renewal is not formally requested.

**4.7.3 Processing certificate renewal requests**

If a Subscriber’s LAWtrust AeSign CA Certificate requires renewal, the LAWtrust AeSign RA that requested renewal of the Subscriber’s LAWtrust AeSign CA Certificate shall make a reasonable effort to notify the Subscriber via a mechanism as described in section 4.1.

**4.7.4 Notification of new certificate issuance to subscriber**

If a Subscriber’s LAWtrust AeSign CA Certificate requires renewal, the LAWtrust AeSign RA that requested renewal of the Subscriber’s LAWtrust AeSign CA Certificate shall make a reasonable effort to notify the Subscriber via a mechanism as described in section 4.1.

**4.7.5 Conduct constituting acceptance of a renewal certificate**

After renewal of the LAWtrust AeSign CA Certificate, the Subscriber shall check that the content of the LAWtrust AeSign CA Certificate is correct.

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

**4.7.6 Publication of the renewal certificate by the CA**


Post renewal the renewed certificate is published in the LAWtrust AeSign CA database.

**4.7.7 Notification of certificate issuance by the CA to other entities**

There are no further communications to other entities.

**4.8 Certificate re-key**

The LAWtrust AeSign CA will re-key a certificate after revocation of the certificate provided that the LAWtrust AeSign RA conducts and confirms that it has conducted the

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

necessary authentication and verification checks for the purposes of the certificate re-key in accordance with the LAWtrust AeSign RA Charter approved by the LAWtrust PA.

#### **4.8.1 Circumstance for certificate re-key**

The LAWtrust AeSign CA 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.
2. a subscriber suspects that access to the private key is compromised.
3. A subscriber has requested that information in the certificate requires amendment.

In the cases described above the subscriber is required to undergo the full registration process in accordance with the LAWtrust AeSign 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 remain unchanged, a new certificate will be issued.

#### **4.8.4 Notification of new certificate issuance to subscriber**

If a Subscriber's LAWtrust AeSign CA Certificate requires re-key, the LAWtrust AeSign RA that requested renewal of the Subscriber's LAWtrust AeSign CA 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 CA Certificate, the LAWtrust AeSign CA Certificate shall be deemed to have been

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

accepted by the Subscriber and the information contained in the LAWtrust AeSign CA Certificate deemed to be accurate.

#### **4.8.6 Publication of the re-keyed certificate by the CA**

Post renewal the renewed certificate is published in the LAWtrust AeSign CA 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 CA Certificates, signed by the LAWtrust Root Certification Authority 2048, contain a Certificate expiration date. When the LAWtrust AeSign CA 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 CA 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 CA Certificate, all Registration Authorities and their Subscribers shall immediately cease using the Certificate and shall remove the LAWtrust AeSign CA Certificate from any devices and/or software in which it has been installed.

### **4.9 Certificate modification**


The LAWtrust AeSign CA shall not modify certificates.

#### **4.9.1 Circumstance for certificate modification**

No Stipulation.

#### **4.9.2 Who may request certificate modification**

No Stipulation.

 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **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.

The LAWtrust AeSign CA will revoke a LAWtrust AeSign CA Certificate after receiving a valid revocation request from any LAWtrust AeSign RA.

A LAWtrust AeSign RA will be entitled to request revocation of and will request revocation of and the LAWtrust AeSign CA will be entitled to revoke and may revoke Subscriber's LAWtrust AeSign CA Certificates, if the LAWtrust AeSign RA or LAWtrust AeSign CA 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 will request revocation of a LAWtrust AeSign CA Certificate if the Subscriber has a suspicion or knowledge of a compromise of the Subscriber's private key or that the


 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

information contained in LAWtrust AeSign CA 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 will be submitted to a LAWtrust AeSign RA and processed according to the processes defined in the LAWtrust AeSign RA Charter (with the Subscriber's application for a new LAWtrust AeSign CA Certificate if applicable).

LAWtrust AeSign 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 CA Certificate issued to a Subscriber;
4. Subscriber suspected of fraudulent activity.
5. The compromise of the LAWtrust AeSign CA 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 CPS or the AeSign Subscriber Agreement entered into with the Subscriber;
7. Non-payment of fees in respect of any services provided by LAWtrust or LT AeSign-RA.
8. Issue or use of the certificate not in accordance with the LAWtrust AeSign 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 exist.
11. The LAWtrust AeSign CA or LAWtrust Root CA 2048 expires.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

12.A determination by the LAWtrust AeSign CA or a LAWtrust AeSign RA that the certificate was not issued in accordance with this LAWtrust AeSign CPS or the provisions of the Subscriber’s Agreement entered into with the Subscriber; or

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

Revocation of a LAWtrust AeSign CA Certificate will not affect any of the Subscriber’s contractual obligations under this LAWtrust AeSign 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 CA Certificate at any time and for any reason.


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

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

**4.10.3 Procedure for revocation request**

A LAWtrust AeSign RA will authenticate a request by a Subscriber for revocation of his/her LAWtrust AeSign CA Certificate by requiring:

**4.10.3.1 Initiate revocation requests**

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

A Subscriber or an approved RA will 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 request will be authenticated by verifying that the requester is the subscriber or an agent of the subscriber who is authorised to request revocation.

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.

The authorised agent of the subscriber will include checking that the agent has a contractual agreement with the LAWtrust AeSign CA and that the agent is authorised to facilitate the issuance of a LAWtrust AeSign CA 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 CA Certificate is revoked for any reason, the LAWtrust AeSign RA that requested revocation of the Subscriber's LAWtrust AeSign CA Certificate will 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 CA certificate revocation lists will be updated as per the schedule specified in section 3.4.4. The serial number of the revoked LAWtrust AeSign CA Certificate will be posted to the CRL located at [[http://aesigncrl.lawtrust.co.za/CRL/lawtrust\\_aesign\\_ca\\_crlfile.crl](http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl)]



 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **4.10.4 Bulk revocation request**

A LAWtrust AeSign RA may request a LAWtrust AeSign CA to revoke LAWtrust AeSign CA Certificates in bulk in accordance with the provision of the relevant LAWtrust AeSign 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 requests**

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

The LAWtrust AeSign CA on receiving the bulk revocation request submitted by the LAWtrust certificate administrator, will determine the timeframes for the bulk revocation using section 3.4.4, process the bulk revocation request and post the serial numbers of the revoked LAWtrust AeSign CA Certificates to the CRL in the LAWtrust repository


[\[http://aesigncrl.lawtrust.co.za/CRL/lawtrust\\_aesign\\_ca\\_crlfile.crl\]](http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl);

Notification and publication of the LAWtrust AeSign CA 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 will initiate a request to revoke the associated LAWtrust AeSign CA Certificate immediately upon detection of the compromise or suspected compromise.

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

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **4.10.6 Time within which LAWtrust AeSign CA must process the revocation request**

The LAWtrust AeSign CA will use commercially reasonable efforts to 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.

#### **4.10.7 Revocation checking requirement for Relying Parties**

Relying parties will check CRL's on a daily basis to ensure reliance on LAWtrust AeSign CA Certificates or 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 PKI CRL issuance frequency is explained in section 3.4.4.


#### **4.10.9 Maximum latency for CRL's**

The maximum LAWtrust AeSign PKI CRL latency is 24 hours in the case where there are no revocations during that 24-hour period.

#### **4.10.10 On-line revocation/status checking availability**

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

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

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **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 key compromise**


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

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

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

#### **4.10.14 Circumstances for suspension**

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

 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

AeSign RA’s Charter or circumstances arise which may result in a revocation (as described in section 4.10.1), is suspected and not confirmed.

#### **4.10.15 Who can request suspension**

A LAWtrust AeSign RA may request a LAWtrust AeSign CA to suspend a LAWtrust AeSign CA Certificate without prior notice to the Subscriber. The LAWtrust AeSign RA will 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 RA Charter, to the eMail address provided in the certificate application.

#### **4.10.16 Procedure for suspension request**

A LAWtrust AeSign RA may request a LAWtrust AeSign CA to suspend a LAWtrust AeSign CA Certificate in accordance with the provision of the relevant LAWtrust AeSign RA Charter as approved by the LAWtrust PA.

The LAWtrust AeSign CA receiving the suspension request will, within 48 hours of receiving such suspension, post the serial number of the suspended LAWtrust AeSign CA Certificate to the CRL in the LAWtrust repository


[http://aesigncrl.lawtrust.co.za/CRL/lawtrust\\_aesign\\_ca\\_crlfile.crl](http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl)

If a Subscriber’s LAWtrust AeSign CA Certificate is suspended for any reason, the LAWtrust AeSign RA that requested suspension of the Subscriber’s LAWtrust AeSign CA Certificate will 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 RA may request the LAWtrust AeSign CA to suspend LAWtrust AeSign CA Certificates in bulk in accordance with the provision of the relevant LAWtrust AeSign RA Charter as approved by the LAWtrust PA.

#### **4.10.16.2 Identifying the certificates to be included in a bulk suspension**

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

The certificates to be included in a bulk suspension are identified by any circumstances as described in section 4.10.14.

#### **4.10.16.3 Procedure for bulk suspension**

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

The LAWtrust AeSign CA on receiving the bulk suspension request submitted by the LAWtrust certificate administrator, will within 48 hours of receiving such suspension request, process the bulk suspension request and post the serial numbers of the suspended LAWtrust AeSign CA Certificates to the CRL in the LAWtrust repository

[http://aesigncrl.lawtrust.co.za/CRL/lawtrust\\_aesign\\_ca\\_crlfile.crl](http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl)


If the Subscribers' LAWtrust AeSign CA Certificates are suspended for any reason, the LAWtrust AeSign RA that requested suspension of the Subscribers' LAWtrust AeSign CA Certificates will 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 RA may suspend a LAWtrust AeSign CA Certificate for a period not exceeding the validity of the LAWtrust AeSign CA Certificate.

#### **4.10.18 Maximum number of allowed suspensions**

There is no limit on the number of allowed suspensions a LAWtrust AeSign RA may place on a LAWtrust AeSign CA Certificate, except if this is specifically stated in a Registration Authority Charter.

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **4.10.19 Who can request the lifting of a certificate suspension**

A LAWtrust AeSign RA may request a LAWtrust AeSign CA to lift the suspension of a LAWtrust AeSign CA Certificate without prior notice to the Subscriber. The LAWtrust AeSign RA will 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 RA Charter, to the eMail address provided in the certificate application.

#### **4.10.20 Procedure for the lifting of a suspension request**

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

#### **4.10.21 Circumstances for lifting certificate suspension**

A certificate is suspended if circumstances arise 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.

### **4.11 Certificate status services**

#### **4.11.1 Operational characteristics**


The LAWtrust AeSign CA 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 CA certificate status services are available 99.98% of the time.

#### **4.11.3 Optional Features**

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

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

The LAWtrust AeSign CA 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 99.98% of the time.

#### **4.12 End of Subscription**

The LAWtrust AeSign CA 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 CA 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 controls**

Entrust software (Security Manager) is used as the software component of the LAWtrust AeSign CA.

#### **5.1.1 Site location and construction**

The LAWtrust AeSign CA hardware and software are hosted in a high security vault in a data centre with physical security and access control procedures that meet or exceed industry standards.

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 5.1.2 Physical access

Physical access to the LAWtrust AeSign CA is strictly controlled. Only authorised LAWtrust representatives may arrange to gain access to the CA’s vault in the data centre 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 CA 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 will be logged and recorded by the data centre security personnel; all the relevant biometric readers and the LAWtrust AeSign CA vault access register.

#### 5.1.2.1 Physical access systems testing

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


### 5.1.3 Network and LAWtrust AeSign CA server security

The LAWtrust AeSign CA hosted in the LAWtrust vault will operate on a dedicated network segment and access to the LAWtrust AeSign CA’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 CA servers.

### 5.1.4 Power and air conditioning

The data centre is provided with power backup and is fully air-conditioned.



 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 5.1.5 Water exposures

The data centre is protected against water exposures.

### 5.1.6 Fire prevention and protection

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

### 5.1.7 Media storage

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

### 5.1.8 Waste disposal

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

### 5.1.9 Off-site backup

Backups are stored at a secure and separate geographic location.


## 5.2 Procedural controls

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

To gain access to the software used by the LAWtrust AeSign CA operational personnel with trusted roles must undergo background checks.

### 5.2.1 Trusted Roles

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

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 5.2.1.1 LAWtrust AeSign CA Roles

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

### 5.2.1.2 Safenet Hardware Security Roles

#### 5.2.1.2.1 Safenet HSM Administrator

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

- Provide login via SSH to SafeNet Luna HSM
- Allows for copying and retrieval of certificates to and from the HSM
- Allows for certain functions to be performed on the HSM


#### 5.2.1.2.2 SafeNet Security Officer

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

- Provide login to the security functions of the HSM
- Allows security functions to be performed on the HSM

#### 5.2.1.2.3 SafeNet Cloning Domain User

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

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

#### 5.2.1.2.4 SafeNet MofN User

The functions of the LAWtrust CA's Safenet HSM MofN User include:

- Provide first time login to the security functions of the HSM with the security officer
- Provide first time activation of the partitions on the HSM
- Provide dual mechanisms on all security functions on the HSM

#### 5.2.1.2.5 SafeNet Partition Owner

The functions of the LAWtrust CA's Safenet 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 SafeNet Luna SA4 HSM. To access the LAWtrust AeSign CA key material a minimum of three HSM administrators are required. To keep the LAWtrust AeSign CA operational, the 3 of 6 scheme is loaded and kept persistent to allow the LAWtrust AeSign CA server access to the private key.

The activation of the LAWtrust AeSign CA key through the SafeNet administrators requires three persons for the LAWtrust AeSign CA. All Entrust roles are assigned strictly according to the prescriptions of the LAWtrust AeSign CA specifications.

#### 5.2.2.1 SafeNet Luna SA4 Hardware Security Module Roles

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### Safenet Luna SA5 Hardware Security Module Roles

- HSM Admin role – 1 of 1
- HSM Security Officers – 3 of 6
- HSM Cloning Domain role – 1 of 2
- HSM Partition Owner / Password– 1 of 1

#### 5.2.2.2 Entrust Security Manager Roles

All roles: either 2 of 3 (first/security officers) or 1 of 3 (master users) or 1 of 1 (Entrust User - Server Administrator).

#### 5.2.3 Roles requiring segregation of duties


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

### 5.3 Personnel controls

The operational personnel for the LAWtrust AeSign CA 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:

1. Control or set CA Policy
2. Set or restore the CA Security Policy
3. Sign Cross Certificates

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### 4. Import certificate definitions/specifications

Operational personnel of the LAWtrust AeSign CA will not be assigned responsibilities that conflicts the segregation of duties requirements of the LAWtrust AeSign CA. The operational personnel for the LAWtrust AeSign CA 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 CA 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 procedures


THE LAWtrust on boarding process includes a background check

1. Employment Reference check
2. Education certificates check
3. Criminal Check

### 5.3.3 Training requirements

LAWtrust personnel performing trusted roles and roles which support the operational infrastructure of the LAWtrust AeSign CA should attend training on the following

1. Underlying hardware infrastructure for server hardware.
2. Operating systems
3. Applications used in the LAWtrust AeSign CA operations

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### 4. 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.

1. Independent contractor agreement
2. Adhere to the LAWtrust Information Security Policies and Procedures.
3. 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

1. LAWtrust information Security Policies
2. LAWtrust induction brochure
3. Information Security awareness training material

 <p>information security solutions   company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 5.4 Audit logging procedures

Significant security events in the LAWtrust AeSign CA 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 CA 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.

## 5.5 Records archival

### 5.5.1 Records to be kept

The LAWtrust AeSign CA 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,

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

#### **5.5.1.4 PKI Database records**

All databases for the LAWtrust AeSign CA are encrypted and protected by The LAWtrust AeSign CA 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, see section 5.1.9

#### **5.5.2 Records Retention Period**

The PKI data listed above is moved from the CA to a NAS at the Data Centre and then moved to an offsite NAS.

The archives of the LAWtrust AeSign CA database are retained for 7 (seven) years.


### **5.6 Key changeover**

Subscribers are issued LAWtrust AeSign CA 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 CA certificate.

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

The LAWtrust AeSign CA 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.



 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 5.7 Compromise and disaster recovery

The LAWtrust AeSign CA has a disaster recovery plan as part of their 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 LAWtrust Registration Authorities, Subscribers or Relying Parties on request. The disaster recovery procedures include the timeframes for recovery as well as information on the location of the disaster recovery site.

LAWtrust requires rigorous security controls to maintain the integrity of the LAWtrust AeSign CA. The compromise of the private key used by the LAWtrust AeSign CA is viewed by LAWtrust 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 Subscribers 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 CA 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 CA 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 CA 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.

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 5.8 LAWtrust AeSign CA or LAWtrust AeSign RA termination

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

In the event that the LAWtrust AeSign CA ceases operation, the LAWtrust AeSign CA Certificate will be revoked by the LAWtrust Root Certification Authority. If LAWtrust believes that there is a risk that the specific LAWtrust AeSign CA private key has been compromised, then LAWtrust will immediately inform AeSign RA's and Subscribers of such a compromise.

## 5.9 LAWtrust AeSign CA impact on third party functionality

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

## 5.10 Escalation of physical security violations

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

# 6. TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation


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

### 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.

 <small>information security solutions company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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**

No Stipulation.

### **6.1.5 Key sizes**

The minimum key size for any LAWtrust AeSign CA is 2048-bit RSA. Currently the LAWtrust AeSign CA has a key size of 2048-bit RSA.

All LAWtrust AeSign Certificates issued shall have a minimum key size of 2048-bit RSA.

The LAWtrust PA will perform an annual review on the LAWtrust AeSign CA 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 CA uses 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 (as per X.509 v3 key usage field)**

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

 <p>information security solutions   company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

1. Digital Signature,
2. Key Encipherment (a0)

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

## **6.2 Private key protection and cryptographic module engineering controls**

### **6.2.1 Cryptographic module standards and controls**

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

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

CA private keys are stored securely using multiple trusted persons to perform sensitive operations.

### **6.2.3 Private key escrow**

LAWtrust AeSign CA does not provide subscriber key escrow.


### **6.2.4 Private key backup**

All LAWtrust AeSign CA private keys are generated and stored by the approved hardware security modules. All keys that are backup up are stored with the same level of protection as keys in production.

### **6.2.5 Private key archival**

LAWtrust AeSign CA All keys that are archived are stored with the same level of protection as keys in production. Private key transfer into or from a cryptographic module

LAWtrust AeSign CA private keys are not transferred out of hardware security modules. Subscriber keys which are generated by hardware security module are encrypted (wrapped) with a Key Encryption Key (KEK) prior to being exported. When required for use the KEK which is stored by the HSM is used to decrypt the subscribers private key.

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 6.2.6 Private key storage on cryptographic module

All LAWtrust AeSign CA private keys are generated and stored by the approved hardware security modules.

## 6.2.7 Method of activating private key

All LAWtrust AeSign CA private keys are activated according to the manufacturers requirements. The detailed activities are scripted and witnessed by at least six trusted personal.

## 6.2.8 Method of deactivating private key

LAWtrust AeSign CA private key deactivation is controlled by the hardware security module authentication mechanism. LAWtrust AeSign CA does not leave private keys activated when not in use.

## 6.2.9 Method of destroying private key

LAWtrust AeSign CA 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.

## 6.2.10 Cryptographic Module Rating


This information is provided for in section 6.2.1.

## 6.3 Other key management aspects

### 6.3.1 Public key archival

The LAWtrust AeSign CA uses software approved by the PA in conjunction with hardware certified to FIPS 140-2 Level 3 to protect the LAWtrust AeSign CA private key. The LAWtrust AeSign CA's private key is backed up and requires a minimum of two HSM key shareholders to be accessed or recovered. The LAWtrust AeSign CA private keys will be destroyed according to the processes set out in the LAWtrust Hardware Disposal Policy.

LAWtrust do not escrow the LAWtrust AeSign CA's private key and no third parties have access to the LAWtrust AeSign CA's private key.


 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

Subscribers are responsible for the generation, protection, backup, archival, recovery, destruction and removal of copies from all systems on destruction (at end of life) of the private key associated with the public key in the LAWtrust AeSign CA Certificate using the mechanisms provided by LAWtrust as documented in the relevant LAWtrust AeSign RA Charters.

### 6.3.2 Certificate operational periods and key pair usage periods

LAWtrust certificates and the maximum validity periods

<b>Certificate</b>	<b>Private Key use</b>	<b>Certificate valid until</b>
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 CA	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	7 February 2023 02:39:23 PM
CRL Signing Certificate:	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
OCSP Signing Certificate:	critical Digital Signature,  Extended Key Usage: critical OCSP Signing	
Time Stamp Authority Certificate	nonRepudiation, digitalSignature  Extended Key Usage: timeStamping	23 November 2018 14:52:06

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b>https://www.lawtrust.co.za/repository</b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

End Entity Certificates Signing	Digital Signature, Non-Repudiation (c0)	Not after 07 February 2022
---------------------------------	---	----------------------------

Table 1: Certificates and the maximum validity periods

Adequate time is allocated for key changeover prior to the maximum validity periods being realised.

## 6.4 Activation data

All LAWtrust AeSign CA private keys are activated according to the manufacturers requirements. The detailed activities are scripted and witnessed by at least six trusted personal.

### 6.4.1 Activation data generation and installation

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

All operational personnel that are authorised to have access to the LAWtrust AeSign CA 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 CA. Physical access to the data

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

centre that hosts the secure vault where the LAWtrust AeSign CA equipment and LAWtrust AeSign CA software are located is described in 5.1.2.

### 6.5.2 Computer security rating

No Stipulation.

## 6.6 Life cycle technical controls

The efficacy and appropriateness of the security settings described in this LAWtrust AeSign 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 controls


No Stipulation.

## 6.7 Network security controls

### 6.7.1 Network and LAWtrust AeSign CA server security

The LAWtrust AeSign CA hosted in the LAWtrust vault will operate on a dedicated network segment and access to the LAWtrust AeSign CA'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 CA servers.



 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 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 CA 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).

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 6.12.1 CA key pair usage

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

## 7. CERTIFICATE PROFILES

LAWtrust digital certificates comply to the X.509 V3 standard. The profile of a LAWtrust AeSign Certificate, approved by the LAWtrust PA, will be governed by the profile given below with minor variations provided for in the LAWtrust AeSign RA Charters.


### 7.1 Certificate profile

#### 7.1.1 Version number(s)


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

#### 7.1.2 Certificate extensions

Field Type	Field Name	Value format	Value	Explanation
	Key Usage	text	Digital Signature, Non-Repudiation (c0)	The purposes for which this certificate can be used.
	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= <a href="http://ocsp.lawtrust.co.za">http://ocsp.lawtrust.co.za</a> [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL= <a href="http://ltadss.lawtrust.co.za/certs/aesignca.cer">http://ltadss.lawtrust.co.za/certs/aesignca.cer</a>	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.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b>https://www.lawtrust.co.za/repository</b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	<p>[1]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.2.1</p> <p>[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  https://www.lawtrust.co.za/repository</p> <p>[1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier:  Notice Text=The certificate policy for LAWtrust Certificates requires subscriber identification and authentication prior to certificate issuance. Certificate verification is performed by a Registration Authority on the certificate applicant according to the verification requirements established by the LAWtrust Policy Authority. 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 .</p>	<p>The LAWtrust documentation governing the CA and certificate usage is published at https://www.lawtrust.co.za/repository.</p> <p>The documentation set includes Policies, Practices and Agreements</p>
	CRL Distribution Points	URL	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL2 CN=LAWtrust AeSign Certification Authority 2048 OU=LAW Trusted Third Party Services PTY Ltd. O=LAWtrust C=ZA</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl</p> <p>URL=ldap://AESIGNCA/cn=LAWtrust%20AeSign%20Certification%20Authority%202048,ou=LAW%20Trusted%20Third%20Party%20Services%20PTY%20Ltd.,o=LAWtrust,c=ZA?certificateRevocationList?base</p>	<p>The LAWtrust AeSign CA will issue CRLs and make them available via 1) http at http://aesigncrl.lawtrust.co.za.</p> <p>2) ldap directory. ldap://hostname:389/cn=CRL&lt;Number&gt;, cn= LAWtrust Root Certification Authority, ou=LAW Trusted Third Party Services PTY Ltd.,o=LAWtrust,c=ZA</p> <p>The CA will issue at least one crl publication by the end of each business day.</p>

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

Field Type	Field Name	Value format	Value	Explanation
	Private Key Usage	Date text	Not before=(day month year hour, minute second) Not after=(day month year hour, minute second)	As per date and time of Issue.
	Authority Key Identifier		KeyID=0e 92 11 7f 10 db b4 be 72 8f e1 b2 b2 df b0 ef 59 5f b9 96	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 keyIdentifier 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=27 80 93 b0 c3 b5 55 12 fa 47 79 b7 1c 2e f6 05 b7 3e 31 c8	The Subject Key Identifier is used by path validation software by helping to identify certificates that contain a particular public key.
	Basic Constraints		Subject Type=End Entity Path Length Constraint=None	Constraints description
	Thumbprint			The digest (or thumbprint) of the certificate data.

### 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	SHA1/RSA		Algorithm to produce signatures
	Signature hash algorithm	sha1		
	Thumbprint Algorithm	sha1		Thumbprint algorithm. The hash algorithm that generates a digest of data (or thumbprint) for digital signatures

### 7.1.4 Name forms

Unique serial numbers are allocated to digital certificates and serial numbers are not recycled.

Subject information inclusive of the Common name is verified as per section 3.

Specific to a subscriber, subscriber OU fields are limited for use by Verified information.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 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=2.16.840.1.114028.10.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:  <a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a>	

### 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

Field Type	Field Name	Value format	Value	Explanation
Policy Qualifier	Certificate Policies	text	[1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=The certificate policy for LAWtrust Certificates requires subscriber identification and authentication prior to certificate issuance. Certificate verification is performed by a Registration Authority on the certificate applicant according to the verification requirements established by the LAWtrust Policy Authority. LAWtrust issues Certificates to subscribers as outlined by the LAWtrust Certification Practice Statement (CPS) which can be found at <a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a> .	

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 7.1.9 Processing semantics for the critical Certificate Policies extension

No Stipulation.

## 7.2 CRL profile

### 7.2.1 Version number(s)

Version: set to v2

### 7.2.2 CRL and CRL entry 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 LAWtrust AeSign CA, ou=LAW Trusted Third Party Services PTY Ltd, O=LAWtrust, C=ZA	
	Effective date		Time of current CRL issuance	
	Next update		Time of next expected CRL issuance	
	Signature algorithm		SHA1	
	Signature hash algorithm		SHA1	
extension	CRL number		unique 32-bit non-negative integer	
extension	Authority key identifier		20 byte SHA-1 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(s)

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

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 7.3.2 OCSF extensions

No Stipulation in addition to Authority Information Access.

## 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The LAWtrust AeSign CA and LAWtrust AeSign RA's will be audited for compliance against the practices and procedures set forth in this LAWtrust AeSign CPS, the WebTrust standard and the SANS21188 standard. This will include:

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

### 8.1 Frequency or circumstances of assessment

The LAWtrust AeSign CA and LAWtrust AeSign RA's will be audited once per calendar year for compliance with the practices and procedures set out above.

### 8.2 Identity/qualifications of assessor


A compliance audit will 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 CA and LAWtrust AeSign RA's will be independent from the Entity being audited.

### 8.4 Topics covered by assessment

The compliance audit will test compliance of the LAWtrust AeSign CA and LAWtrust AeSign RA's against the requirements set out above.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 8.5 Actions taken as a result of deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited LAWtrust AeSign CA or LAWtrust AeSign RA will use commercially reasonable efforts to correct any such deficiencies in an expeditious manner, taking into account the risk/severity of the non-conformance and the commercial impact of the remediation.

## 8.6 Communication of results

The result of all compliance audits will 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 CA 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 CA 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.



 <p>information security solutions company www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 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

No Stipulation.

### 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.lawtrust.co.za/pages/privacy-notice>
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

 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

- Professional Indemnity
- Cyber Liability
- Directors and Officers Liability

### 9.2.2 Other assets

No stipulation.


### 9.2.3 Insurance or warranty coverage for end-entities

## 9.3 Confidentiality of business information

LAWtrust will not use, disclose or sell Applicant or Subscriber information, except in accordance with this LAWtrust AeSign CPS, Subscriber Agreement or Relying Party Agreement. LAWtrust and LAWtrust AeSign 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 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 CA Certificate Application is incorporated into a LAWtrust AeSign CA Certificate and that the LAWtrust AeSign CA, LAWtrust AeSign 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 CA Certificate, and which is not included in the information described in 9.3.2 below, shall be considered to be confidential. The LAWtrust AeSign CA and LAWtrust AeSign 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 CA Certificate Applications or that are assisting LAWtrust in the operation of the LAWtrust AeSign CA or LAWtrust AeSign RA’s. Information considered to be confidential shall not be disclosed unless compelled, pursuant to legal,

 information security solutions company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

judicial or administrative proceedings, or otherwise required by law. The LAWtrust AeSign CA and LAWtrust AeSign 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 CA Certificate or a LAWtrust Revocation List shall not be considered confidential.


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

### 9.3.3 Responsibility to protect confidential information

LAWtrust, and LAWtrust AeSign 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 CPS, Subscriber Agreements or Relying Party Agreements.

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 9.4 Privacy of personal information

Privacy of personal information shall be protected in terms of the LAWtrust Privacy Notice published on the LAWtrust Website at [<https://www.lawtrust.co.za/pages/privacy-notice>].

### 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

LAWtrust deems all information regarding digital certificate applications, issuance which is not in the public domain as private.

### 9.4.3 Information not deemed private

Information published in digital certificates, and certificate status mechanisms are not deemed as private.

### 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

Information published in digital certificates is done so with prior consent from the applicant.

### 9.4.6 Disclosure pursuant to judicial or administrative process

In the case where LAWtrust are required by law of regulations to disclose information, it will do so without prior consent.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### 9.4.7 Other information disclosure circumstances


No stipulation.

#### 9.5 Intellectual property rights

LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under all LAWtrust AeSign CA Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in a LAWtrust AeSign CA Certificate, which information shall remain the property of the Applicant or Subscriber. All Applicants and Subscribers grant to LAWtrust and any LAWtrust AeSign RA’s operating under the LAWtrust AeSign CA a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under this LAWtrust AeSign CPS, any Subscriber’s Agreement, and any Relying Party Agreements. LAWtrust grants to Subscribers and Relying Parties a non-exclusive, non-transferable license to use, copy, and distribute LAWtrust AeSign CA Certificates, subject to such LAWtrust AeSign CA Certificates being used as contemplated under this LAWtrust AeSign CPS, Subscriber’s Agreement, and any Relying Party Agreements, and further provided that such LAWtrust AeSign CA Certificates are reproduced fully and accurately and are not published in any publicly available database, repository, or directory without the express written permission of LAWtrust. Except as expressly set forth herein, no other right is or shall be deemed to be granted, whether by implication, estoppels, inference or otherwise. Subject to availability, LAWtrust may in its discretion make copies of one or more Cross Certificate(s) available to Subscribers for use solely with the LAWtrust AeSign CA Certificate issued to such Subscribers. LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Cross Certificate(s).

LAWtrust grants permission to reproduce this LAWtrust AeSign CPS provided that:

- The copyright notice on the first page of this LAWtrust AeSign CPS is retained on any copies of the LAWtrust AeSign CPS; and

 <p>information security solutions   company</p> <p>www.lawtrust.co.za</p>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

- This LAWtrust AeSign CPS is reproduced fully and accurately. LAWtrust retains all right, title, and interest (including all intellectual property rights), in, to and under this LAWtrust AeSign CPS.

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


## 9.6 Representations and warranties

LAWtrust makes the following limited warranties to Subscribers with respect to the operation of LAWtrust AeSign CA:

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

Notwithstanding the foregoing, in no event does LAWtrust, or any LAWtrust AeSign RA or the employees, or directors of LAWtrust or a LAWtrust AeSign RA 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 CA Certificate, including,

 information security solutions   company www.lawtrust.co.za	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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 CA Certificate,
- Any software whatsoever, or
- Non-repudiation of any LAWtrust AeSign CA Certificate or any transaction facilitated through the use of a LAWtrust AeSign CA Certificate, since such determination is a matter of applicable law.


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

### **9.6.1 CA representations and warranties**

The same liability provisions that apply in Section 9.6 with respect to LAWtrust AeSign CA shall apply with respect to LAWtrust AeSign RA’s and employees, and directors of the foregoing.

### **9.6.2 RA representations and warranties**

LAWtrust appointed RA’s identity verification and certificate lifecycle management are in conformation to the LAWtrust CP and CPS.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 9.6.3 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 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 CA Certificate Application was created using sound cryptographic techniques and has not been compromised;
- Any information provided to LAWtrust or to a LAWtrust AeSign RA by the Applicant or Subscriber in connection with a LAWtrust AeSign CA 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 RA to which it submitted a certificate application as soon as practicable if any information included in the Applicant’s LAWtrust AeSign CA Certificate Application changes or if any change in any circumstances would make the information in the Applicant’s LAWtrust AeSign CA Certificate Application misleading or inaccurate;
- The Subscriber shall immediately cease to use the Subscriber’s LAWtrust AeSign CA Certificate if any information included in the Subscriber’s LAWtrust AeSign CA Certificate changes or if any change in any circumstances would make the information in the Subscriber’s LAWtrust AeSign CA Certificate misleading or inaccurate;
- The Subscriber shall immediately cease to use the Subscriber’s LAWtrust AeSign CA Certificate upon:

Expiration, suspension or revocation of the Subscriber’s LAWtrust AeSign CA Certificate, or

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



 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

#### **9.6.4 Relying party representations and warranties**

Relying Parties represent and warrant to LAWtrust that:


- The Relying Party shall properly validate a LAWtrust AeSign CA Certificate before making a determination about whether to rely on such LAWtrust AeSign CA Certificate, including confirmation that the LAWtrust AeSign CA Certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root;
- The Relying Party shall not rely on a revoked or expired LAWtrust AeSign CA Certificate;
- The Relying Party shall not rely on a LAWtrust AeSign CA Certificate that cannot be validated back to a trustworthy root;
- The Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on a LAWtrust AeSign CA Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by a LAWtrust AeSign CA Certificate and the importance or value of any transaction that may involve the use of a LAWtrust AeSign CA Certificate; and
- The Relying Party shall not use a LAWtrust AeSign CA Certificate for any hazardous or unlawful (including tortuous) activities.

#### **9.6.5 Representations and warranties of other participants**

No Stipulation.

#### **9.7 Disclaimers of warranties**

Except as specifically provided in sections 9.6 and 9.6.1, neither LAWtrust, the LAWtrust AeSign CA nor any LAWtrust AeSign RA 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 all LAWtrust AeSign RAs and the employees, and directors of the foregoing specifically disclaim any

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

and all representations, warranties, and conditions of merchantability, non-infringement, title, satisfactory quality, and/or fitness for a particular purpose.

## 9.8 Limitation of liability

Neither LAWtrust, nor any LAWtrust AeSign RA, 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 vi the appointed RA's or via the LAWtrust repository.

 <small>information security solutions company</small> <a href="http://www.lawtrust.co.za">www.lawtrust.co.za</a>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

## 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 CA or a LAWtrust AeSign 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 CPS, any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or LAWtrust AeSign 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 RA.
- A proposal for an amendment to this LAWtrust AeSign CPS or to any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or LAWtrust AeSign 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. See sections 1.5.4.2 and 1.5.4.3 for more detail.
- 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.

 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

### 9.12.3 Circumstances under which OID must be changed

The Policy Authority determines whether CPS changes require and amendments.


### 9.13 Dispute resolution

In cases of legal or 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 an advocate practising at the Johannesburg Bar 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 Chairman at the time of the Johannesburg Bar Council 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 CPS and any Subscriber’s Agreement or Relying Party Agreement entered into pursuant to this LAWtrust AeSign CPS shall be governed by and construed in accordance with the laws of the Republic of South Africa. Furthermore, the parties hereto irrevocably and unconditionally consent to the non-exclusive jurisdiction of the Johannesburg Magistrate’s Court or the South Gauteng

 <small>information security solutions   company</small> <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

Division of the High Court of South Africa, as the case may be, in regard to the enforcement of any rights relating to all matters arising from this LAWtrust AeSign CPS.

### **9.15 Compliance with applicable law**

This CPS is subject to all applicable laws and regulations including the Electronic Communications and Transactions Act of 2002 and the South African Accreditation Authority Regulations.

### **9.16 Miscellaneous provisions**

#### **9.16.1 Entire agreement**


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

#### **9.16.2 Assignment**

Any entity operating under this CPS may not assign their rights or obligations to any party without written consent by LAWtrust.

#### **9.16.3 Severability**

To the extent that any provisions of this LAWtrust AeSign CPS or Subscriber or Relying Party Agreements, as the case may be, may be struck-out as unlawful, only those provisions shall be severed from this LAWtrust AeSign CPS or a Subscriber or Relying Party Agreements and all other provisions of this LAWtrust AeSign CPS or Subscriber or Relying Party Agreements shall remain of full force and effect, notwithstanding the severing of those provisions. Any warranties for the service that are affected by corporate activity will be addressed in MSA's with Registration Authorities where necessary.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

#### **9.16.4 Enforcement (attorneys' fees and waiver of rights)**

Any fees or costs awarded in terms of litigation or any other process resulting from Enforcement of this agreement will be governed by the decision of the presiding body, whether in terms of section 9.13 of this CPS or an order of a court in terms of section 9.14


#### **9.16.5 Force Majeure**

Neither LAWtrust, nor any LAWtrust AeSign RA, 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 this LAWtrust AeSign CPS, any Subscribers Agreement, 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**

The LAWtrust AeSign CPS, the Subscriber Agreements, and the Relying Party Agreements state all of the rights and obligations of LAWtrust, any independent third-party Registration Authorities operating under a LAWtrust Certification Authority, any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing, and any Applicant, Subscriber, or Relying Party and any other persons, entities, or organizations in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications, or understandings of any nature whatsoever whether oral or written.

 <b>www.lawtrust.co.za</b>	<b>Classification</b>	<b>LEVEL 1: PUBLIC INFORMATION</b>
	<b>Reference</b>	<b>LT_ISP_IS_AES_CPS_VI05_2018-12-12</b>
	<b>Location</b>	<b><a href="https://www.lawtrust.co.za/repository">https://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>VI05 2018-12-12</b>
	<b>Policy Authority</b>	<b>LAWtrust PA</b>

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

## 10. SIGN OFF ACCEPTANCE

<b>Name:</b>	Katekani Hlabathi
<b>Authority:</b>	Policy Authority
<b>Title:</b>	Chief Information Officer
<b>Date:</b>	2018-12-12
<b>Signature:</b>	