

| | | |
|---|-------------------------|--|
|  <p>information security solutions company</p> <p>www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

LAWtrust Certificate Policy

Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07

("LAWtrust")

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

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

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

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


| | | |
|---|-------------------------|--|
|  <p>information security solutions company</p> <p>www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

COPYRIGHT NOTICE

LAW TRUSTED THIRD PARTY (PTY) LTD (“LAWTRUST”) RETAINS THE COPYRIGHT IN THIS CERTIFICATE POLICY (“CP”) 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.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

DOCUMENT CONTROL

Document history

| Version Number | Effective Date | Author | Summary of Changes | Status |
|-----------------|----------------|----------------|---|-------------|
| V01 13-02-2007 | 13-02-2007 | B Anderson | Review | Expired |
| V02 17-05-2010 | 17-05-2010 | N van Greunen | Review | Expired |
| V03 06-12-2013 | 06-13-2013 | N van Greunen | Logo changes and Review | Expired |
| V04 05-12-2014 | 05-12-2014 | N van Greunen | Review | Expired |
| V05 18-11-2015 | 01-12-2015 | B Anderson | Review | Expired |
| V006 2016-12-21 | 2016-12-21 | Bruce Anderson | Amended logo, approval Signature, Updated Certificate profiles | Expired |
| V007 2017-02-21 | 2017-02-21 | B Anderson | Amendments as per Audit requirements | Expired |
| V008 2017-09-28 | 2017-10-01 | B Anderson | Annual Review | Expired |
| V009 2018-06-15 | 2018-06-15 | Bruce Anderson | Annual Review, amended (identity document definition & governing law) | Expired |
| V010 2018-08-06 | 2018-08-06 | B Anderson | Added Housekeeping items | Expired |
| V011 2018-12-14 | 2018-12-14 | E Oosthuizen | Apply new document template, Address change | Expired |
| V012 2019-03-08 | 2019-03-08 | E Oosthuizen | Review and Housekeeping items | Operational |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

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 | https://www.lawtrust.co.za/repository |
| 2 | LAWtrust AeSign CEN-SSCD RA Charter | https://www.lawtrust.co.za/repository |
| 3 | LAWtrust Relying Party Agreement | https://www.lawtrust.co.za/repository |
| 4 | LAWtrust Subscriber Agreement | https://www.lawtrust.co.za/repository |
| 5 | LAWtrust Privacy Policy | https://www.lawtrust.co.za/pages/privacy-notice |
| 6 | LAWtrust mPKI Services Agreements | LAWtrust & Registration Authorities |



| | | |
|--|-------------------------|--|
|  Lawtrust an ETION <small>information security solutions company</small> www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

TABLE OF CONTENTS

| | |
|--|-----------|
| 1. PURPOSE | 7 |
| 2. SCOPE | 8 |
| 3. POLICY STATEMENT | 9 |
| 3.1 LAWtrust CPS | 9 |
| 3.2 Digital certificate intended usage..... | 9 |
| 3.3 Subscriber identification and authentication | 9 |
| 3.4 Publication of a digital certificate status..... | 9 |
| 3.5 Subscriber private key protection | 10 |
| 3.6 Issuer private key protection..... | 10 |
| 3.7 X509 V3 Mandatory Field requirements | 10 |
| 4. OBLIGATIONS AND LIABILITIES | 10 |
| 4.1 Issuer | 11 |
| 4.2 Relying Party | 11 |
| 5. SECURITY MANAGEMENT | 12 |
| 5.1 Policy Structure..... | 12 |
| 5.2 Policy Administration..... | 12 |
| 6. GOVERNING LAW..... | 13 |
| 7. APPENDIX A [Digital Certificate Specification] | 14 |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

7.1 LAWtrust Root CA 204814

7.2 LAWtrust2048 CA216

7.3 LAWtrust AeSign CA118


7.4 LAWtrust AeSign CA221

7.5 LAWtrust AATL CA123

7.6 LAWtrust LTCA204826

8. APPENDIX B (Definitions).....29

9. SIGN OFF ACCEPTANCE.....40

| | | |
|---|-------------------------|--|
|  <p>information security solutions company</p> <p>www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

1. PURPOSE

Law Trusted Third Party Services (Pty) Ltd (“LAWtrust”) [<https://www.lawtrust.co.za>] conducts the business of providing trusted third-party authentication and public key cryptography services.

LAWtrust manage and operate two PKI hierarchies offering certification services from the LAWtrust managed issuing CA’s to their clients.

1. the LAWtrust root and all issuing CA’s signed into that hierarchy and
2. the single issuing CA which is signed into the Entrust root.

These services include:

1. appointing third party customer Registration Authorities (“RA”),
2. training and monitoring certificate administrators appointed by RA(s),
3. the issuing of digital certificates by the certificate authorities it operates (“LAWtrust Root CA”, “LAWtrust AeSign CA1”, “LAWtrust AeSign CA2”, “LAWtrust AATL CA01”, LAWtrust2048 CA2 and the “Entrust chained CA”)
4. managing the lifecycle of digital certificates issued,
5. providing reference information on the status of all digital certificates issued.

Digital certificates, containing a public key, identify the person who is the holder of the associated private key used to digitally sign an electronic transaction. This forms the basis of positive identity, message integrity, and non-repudiation when conducting business electronically. Private keys may also be used to achieve confidentiality.

This LAWtrust Certificate Policy introduces the rules that LAWtrust requires adherence to in order to ensure a high level of trust in the digital certificates issued by the LAWtrust CA(s). Digital certificates, properly issued, are an effective risk management tool used address the business need for positive identity, privacy and non-repudiation.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

2. SCOPE

The management of the resources required to operate the LAWtrust CA(s) is in accordance with the provisions contained in the LAWtrust Certification Practice Statements ("LAWtrust CPS(s)").

These resources include registration authorities, personnel, network infrastructure, IT systems, cryptographic material, physical locales, and information assets.

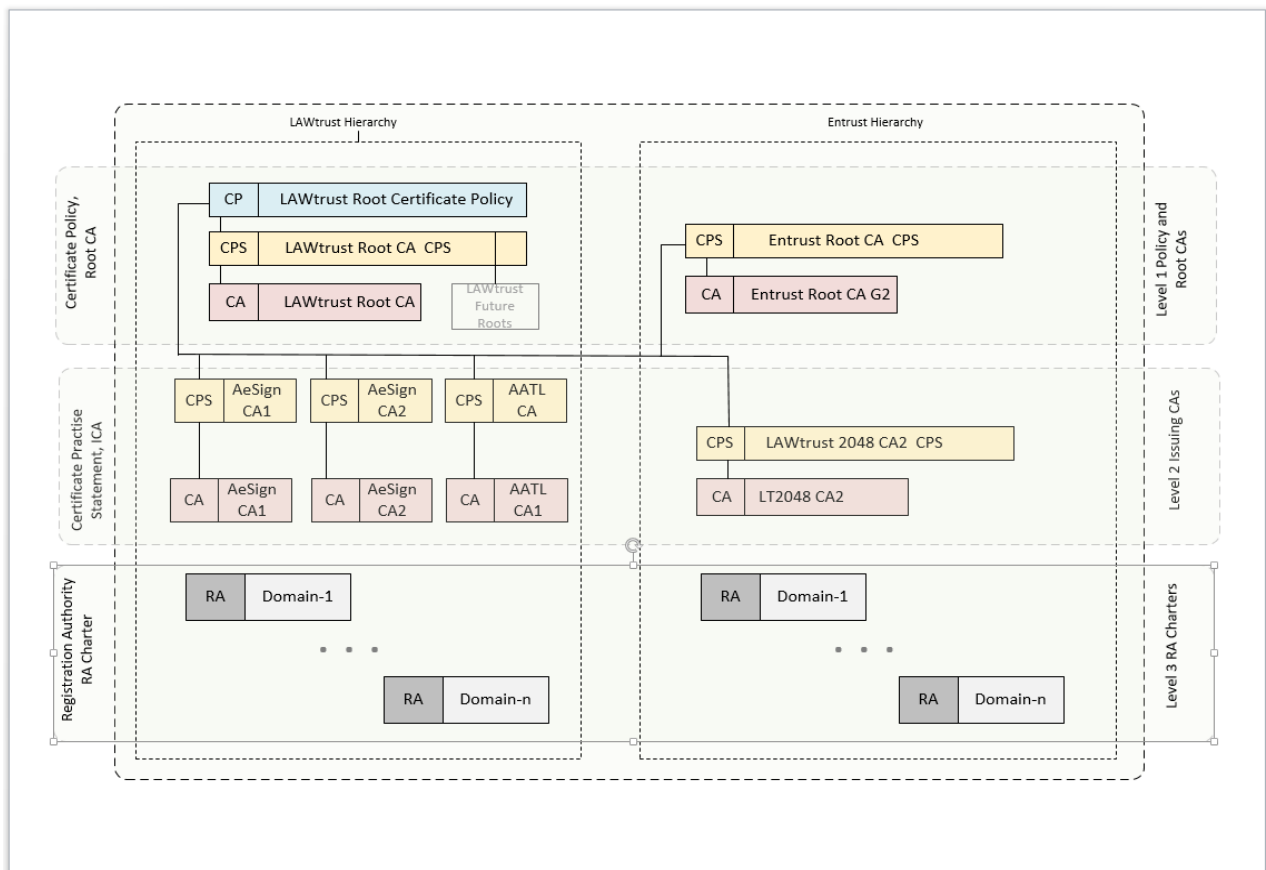


Figure 1: Certification Authorities and Governance documents of LAWtrust PKI

The two hierarchies managed by LAWtrust are shown in the diagram above. The LAWtrust chained hierarchy and the Entrust Chained hierarchy. This Certificate Policy provides the Policy statements for both hierarchies within the LAWtrust PKI. The Root CA has a dedicated CPS and each issuing CA chained into the root CA has their own dedicated CPS.

The Entrust chained CA has a dedicated CPS which is compliant to this LAWtrust CP.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

3. POLICY STATEMENT

3.1 LAWtrust CPS

All digital certificates are issued in accordance with the LAWtrust Certification Practice Statements ("LAWtrust CPS(s)") and LAWtrust Registration Authority Charters ("LAWtrust RA Charters"). The LAWtrust CPS(s) define the practices and procedures that LAWtrust and/or customer RA(s) employ in identification, authentication, issuing, managing, revoking, and renewing digital certificates. The LAWtrust CPS(s) are based on the LAWtrust Certificate Policy, the practices and policies of Entrust, Inc. [<http://www.entrust.com>], the Electronic Communication and Transactions Act, 2002, international public key infrastructure standards (e.g. PKCS for X509 v.3 format certificates), LAWtrust's Information Security Policies (i.e. enterprise, system specific, and issue specific policies), LAWtrust's shareholder requirements, and most importantly LAWtrust's customer requirements.

3.2 Digital certificate intended usage

Digital certificates issued by the LAWtrust Issuing CA(s) are intended for the following purposes: (i) prove identity to a remote information system, (ii) protecting email messages, (iii) Online Certificate Status Protocol (OCSP) response signing, (iv) Entrust Event certificate signing, (v) PKIX-CMP signing, (vi) smart card Logon, (vii) encryption and signing purposes. All digital certificates issued by LAWtrust may only be used for lawful purposes.

3.3 Subscriber identification and authentication

A subscriber is required to: (i) complete and sign a personal digital certificate application form and a Subscriber Agreement; (ii) present his/her identity document, to a certificate administrator. The application and identity verification processes are outlined in each of the CPS's and the specific LAWtrust RA Charter. After authenticating the identity of the subscriber, the information contained in the personal digital certificate application form, and the signatures of the subscriber on the personal digital certificate application form and the Subscriber Agreement, the LAWtrust RA will request the LAWtrust CA(s) to issue a digital certificate to the subscriber.

3.4 Publication of a digital certificate status

The status of a digital certificate issued by the LAWtrust CA(s), i.e. information on whether a digital certificate has been revoked and at what time, appears in the LAWtrust certificate

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

revocation lists, as updated from time to time. References to the CRLs are published in the LAWtrust Relying Party Agreement located in the LAWtrust Repository, located at <https://www.lawtrust.co.za/repository>. The latest version will be available showing the date of publication in the document name, LAWtrust-Relying-Party-Agreement.

3.5 Subscriber private key protection

A Subscriber is required to protect the access to the private key associated to the digital certificate issued by the LAWtrust CA(s) by maintaining the confidentiality thereof. This may include: (i) using adequate password controls, (ii) up to date antivirus/spyware protection mechanisms, (iii) data backups, (iv) cryptographic tokens to store the private key, (v) rely on LAWtrust for the secure generation and storage of their private key.

3.6 Issuer private key protection

LAWtrust appreciates the importance of guarding against the risk of compromise of a CA(s) private key(s) and, as such, implements appropriate controls to ensure the continued security of its CA(s) private key(s). An outline of these measures is published in the LAWtrust CPS(s). Such mechanisms include: (i) the private key material must be stored inside a hardware security module, (ii) all cryptographic operations will be performed inside of a hardware security module, (iii) access to sensitive operations on the hardware security module is restricted and controlled via segregation of duties, (iv) all personnel participating in sensitive cryptographic functions will have undergone reasonable clearance procedures in order to establish a high level of trust.


3.7 X509 V3 Mandatory Field requirements

The following LAWtrust CA(s) digital certificate fields are set out in Annexure A in this document: Version Number, Serial Number, Signature Algorithm, Issuer, Validity Dates, Subject, Public Key Algorithm, Public Key Minimum Length, and other appropriate fields, for example any Required Extensions.

4. OBLIGATIONS AND LIABILITIES

4.1 Subscriber

All obligations and liabilities of a subscriber, i.e. the person applying to be issued with a digital certificate, are governed by the terms and conditions contained in the LAWtrust Subscriber

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


Agreement, which includes: (i) providing and guaranteeing the accuracy of information in a certificate application and the acceptance of a certificate, (ii) protecting the access to the private key associated to the certificate issued, (iii) notification of private key compromise or change of status, (iv) restrictions of the use of the certificate to the usage specified, and (v) ensuring relying parties are made aware of the provisions of any applicable relying party agreement. The most recent copy of the Subscriber Agreement(s) is available for download from the LAWtrust website. You may consider the versions of the Subscriber Agreement(s) available for download from the LAWtrust website [<https://www.lawtrust.co.za/repository>] as the most current versions as at the time of downloading.

4.1 Issuer

All obligations and liabilities of the Issuer, i.e. the LAWtrust CA(s) and/or LAWtrust RA(s) including the certificate administrator(s), are governed by provisions contained in the LAWtrust CPS(s) and/or LAWtrust RA Charters, which include: (i) notification that a certificate has been revoked, (ii) making available certificate status to relying parties (certificate revocation list), (iii) being audited for compliance against stipulated practices and procedures, (iv) disclaimers and limitation of liability, and (v) confidentiality protection to non-public subscriber and relying party information. The most recent copies of the LAWtrust CPS(s) are available for download from the LAWtrust website. You may consider the versions of the LAWtrust CPS(s) available for download from the LAWtrust website [<https://www.lawtrust.co.za/repository>] as the most current versions as at the time of downloading. If permission was granted by the appointed LAWtrust RA, the most recent copies of the LAWtrust RA Charters are available for download from the LAWtrust website. These Charters are also available on the intranets of the applicable RA(s).

4.2 Relying Party

All obligations and liabilities of a relying party, i.e. a person (recipient) who has received a digitally signed data message and is relying on the contents of a digital certificate and the digital signature to (i) identify the person who signed that message, and (ii) confirm the correctness (integrity) of the contents of the message itself, are governed by the terms and conditions contained in the LAWtrust Relying Party Agreement, which includes: (i) applicable usage, (ii) liability exclusions, limitations and warranties, and (iii) validating the digital signature and its associated digital certificate.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

5. SECURITY MANAGEMENT

LAWtrust manages its information security through an information security management program (“ISMP”). Two authoritative bodies comprising of senior management have been established to manage the LAWtrust CA environment. The LAWtrust Policy Authority (“LAWtrust PA”) is responsible for all policy administration; such policies include the LAWtrust CP, CPS(s) and RA Charters. The LAWtrust Operating Authority (“LAWtrust OA”) is the body responsible for the operational implementation of the CPS(s) and RA Charters. This includes all procedures and standards required to ensure correct implementation of the CPS. The CPS(s) are based on this Certificate Policy and supported by information security policies established by the LAWtrust PA.

5.1 Policy Structure

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


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

Certificate Authority Specific Polices: (Including Certificate Policy, Certificate Practice Statements and RA Charters)

Please refer to Figure 2: Certification Authorities and Governance documents of LAWtrust PKI in section 2 of this CP for an understanding of the PKI policies involved.

5.2 Policy Administration

A LAWtrust Policy Authority (“LAWtrust PA”) is set up to manage the lifecycle of the Certificate Policy. The LAWtrust Operating Authority (“LAWtrust OA”) is setup to ensure that the practices and controls specified in the CPS(s) fully support the CP. The LAWtrust PA may, from time to time, amend the provisions of this CP. The LAWtrust PA may be contacted on governance@lawtrust.co.za.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

6. GOVERNING LAW


This document will be governed by the laws of the Republic of South Africa in as far as it relates to the operations or actions of LAWtrust in terms of this document.

This document will also be governed by the laws of the country in which the applicant is a citizen or normally resides.

In the event of a dispute between the certificate holder and a person or entity in the country of residence or origin of the certificate holder, such disputes will be dealt with by the laws of said country.

In the event of a dispute between LAWtrust and a certificate holder that is not resident in or a citizen of the Republic of South Africa, such a dispute will be dealt with in accordance with the Rules of the London Court of Arbitration, which will function as a neutral jurisdiction between the parties.


It is the duty of the applicant for a digital certificate to ensure that the usage of such a certificate is valid and legal in the country where the applicant intends using it.

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

7. APPENDIX A [Digital Certificate Specification]


7.1 LAWtrust Root CA 2048

| LAWtrust Root CA 2048 Certificate Profile Summary Table (part 1) | | | |
|--|--------------------------|---|---|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 4F B3 D0 EE | The LAWtrust Root CA 2048 unique serial number. |
| | Signature Algorithm | sha1RSA | Algorithm to produce signatures |
| | Issuer | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd O = LAWtrust C = ZA | Entries describing the Issuer in terms of the DN. |
| | Valid from | Not valid before date (Wednesday, May 16, 2012 5:40:18 PM) | |
| | Valid to | Not valid after date (Sunday, May 16, 2032 6:10:18 PM) | |
| | Subject | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd O = LAWtrust C = ZA | Subject details of the Root CA certificate. This uniquely identifies the LAWtrust Root CA 2048. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 a4 dc 91 b1 0a 15 1e 36 ae 11 44 45 97 d5 25 35 87 8b 1b 0a d1 cf 70 fa 26 41 b1 fc 4a 0d a8 5a b5 66 a7 dc 1f 6e 1d 08 e9 a6 86 0b 66 44 5c b8 50 a2 30 96 02 0b 88 c8 15 54 17 af fa d7 e4 6a 0f 80 c7 ce e5 e8 a6 99 b2 4b 7f 92 4d 36 65 54 ee 21 30 23 e4 0f c7 42 e7 5d cc 2f 1b 3e 6b 0a a7 3e d1 8f 07 2e d8 b7 fa cf 18 55 35 99 b3 d0 52 bb 0d e7 a9 4b 1b fb fb 46 ff 01 09 b2 37 4f b1 fd 79 3a f8 36 ec 63 2a dc fb 38 f1 b7 e8 61 e0 91 d2 bb 78 15 36 74 bd 1d b5 5e d9 bd b6 6e 08 fc 79 f6 ba 7f e4 1c 2d 40 bd 1d b6 03 a4 02 c8 eb 6a 18 db 77 65 67 b5 93 6a 3a e0 dd 24 57 ab 81 e2 fd 71 d7 d7 5e ed 8e fc 60 c5 e7 b9 fc 23 a6 b9 6b f7 dc d3 26 02 9a 6e e0 03 85 fb c5 a7 c6 51 ec c9 69 13 f4 16 0b ed 34 01 22 23 7b dd 2b 41 96 a9 3a 4c ea 6a 57 75 2b 0b 0f 14 3f 02 03 01 00 01 | The public Key unique to the LAWtrust Root CA 2048 |
| | Key Usage | Certificate Signing, Off-line CRL Signing, CRL Signing (06) | Specifies practical usages of the LAWtrust Root CA certificate |
| | Private key usage period | Not before=Wednesday, May 16, 2012 5:40:18 PM Not after=Sunday, May 16, 2032 6:10:18 PM | Dates within which the private key is valid. |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

LAWtrust Root CA 2048 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|---|--|
| Certificate Extensions | CRL Distribution Points | <p>[1] CRL Distribution Point</p> <p>Distribution Point Name: Full Name:</p> <p>URL= http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl</p> <p>[2] CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>Directory Address:</p> <p>CN=CRL1</p> <p>CN=LAWtrust Root Certification Authority 2048</p> <p>OU=LAW Trusted Third Party Services PTY Ltd.</p> <p>O=LAWtrust</p> <p>C=ZA</p> | <p>The LAWtrust Root CA 2048 will issue CRLs and make them available via http and ldap directory.</p> <p>The CA will issue at least one crl every 6 months.</p> |
| | Authority Key Identifier | KeyID=5c de 3a 33 34 49 64 c4 92 31 7c 55 5e f5 f2 3b 4f ee c3 1d | The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number. |
| | Subject Key Identifier | KeyID=93 da eb 6d 26 34 ac 2e af 3d 55 74 1e 4c 82 c1 d8 a8 da cb | 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=CA Path Length Constraint=None | Constraints description |
| | Entrust Version Info | Entrust Authority Security Manager Version=V8.2 | Information specifying the Version of the Entrust Security Manager Software |
| Certification Hierarchy | Certification Path | Self-signed LAWtrust Root Certification Authority 2048 | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

7.2 LAWtrust2048 CA2

| LAWtrust2048 CA2 Certificate Profile Summary Table (part 1) | | | |
|---|--------------------------|---|---|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 61 3d 38 bf 00 00 00 00 51 d3 71 90 | The LAWtrust2048 CA2's unique serial number. |
| | Signature Algorithm | SHA2/RSA | Algorithm to produce signatures |
| | Issuer | CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US | Entries describing the Issuer in terms of the DN. |
| | Valid from | 20 May 2015 05:37:57 PM | |
| | Valid to | 20 May 2025 06:07:57 PM | |
| | Subject | CN = LAWtrust2048 CA2 O = LAWtrust C = ZA | Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust2048 CA2. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 cd 6f c1 7f 51 71 56 8a e2 7a 61 bc c9 00 78 0d ff a0 49 e4 09 1e e5 7d 38 84 5a 2a 71 d2 6e 97 8c be 8f e5 58 7e 03 a2 a6 5a 57 a9 b3 df 8d 8c 23 fb 59 72 d0 9f 95 97 e2 12 54 7f 4e ae 00 a6 90 2b 82 38 80 c5 0c 5b 5d 9d bc 32 c2 79 2a 98 9f 7c de 45 67 26 42 78 5b 0f d2 d2 9c 49 53 31 cf 73 5d e4 67 f0 d4 f5 bd 28 9c f3 33 ba 96 4e fb 29 fa 77 df 82 3d 42 be 70 11 79 37 68 3d ea 2c 77 f0 08 6a 66 5b 0b 98 c1 c7 01 3d 2f ec 7b 9f 01 79 97 e9 f5 5e cf 07 85 f3 21 f0 97 fd 6b 0c 24 5f e6 57 10 92 53 0b 88 fd 6a 0a a1 97 e7 14 01 b9 75 57 59 1a cb aa 83 88 a7 cd 5b d6 7e 11 81 f4 5e 8a 3d 09 06 63 4b 23 25 51 4c 53 4b 6e 7f 46 28 82 75 3d 34 70 83 ec 98 ba 88 6b 05 fb eb 95 26 ce 74 3e 3b cd b5 8f 11 41 25 8d a6 0a 79 34 bf f5 30 4f 38 6e 0e 04 86 5f 65 56 e1 02 03 01 00 01 | The public key of the LAWtrust2048 CA2. |
| | Key Usage | Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86) | Specifies practical usage of certificate |
| | Enhanced Key Usage | Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) Entrust Event Certificate Signing (2.16.840.1.114027.40.3) Unknown Key Usage (2.16.840.114027.40.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) | |
| | Private key usage period | Not before= 20 May 2015 05:37:57 PM Not after= 20 May 2025 06:07:57 PM | Dates within which the private key is valid. |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust2048 CA2 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|--|--|
| Certificate Extensions | CRL Distribution Points | [1]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.1.8 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/cps [2]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.2.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.lawtrust.co.za/repository | The LAWtrust documentation governing the CA and certificate usage is published at https://www.lawtrust.co.za/repository . The documentation set includes Policies, Practices and Agreements |
| | CRL Distribution Points | [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.entrust.net/g2ca.crl | The LAWtrust2048 CA2 will issue CRLs and make them available via 1] http://2048crl.lawtrust.co.za/CRL/lawtrust2048_ca2_lawtrust_za_crlfile.crl |
| | Authority Key Identifier | KeyID=6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab | The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number. |
| | Subject Key Identifier | KeyID=73 dc 15 6d ab 44 e6 a2 7e ea e9 f6 f0 bc c8 f0 36 16 bb 4b | 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=CA Path Length Constraint=0 | Constraints description |
| | Entrust Version Info | Not Specified | Information specifying the Version of the Entrust Security Manager Software |
| Certification Hierarchy | Certification Path | Entrust Root Certification Authority - G2 ↳ LAWtrust2048 CA2 | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


7.3 LAWtrust AeSign CA1

| LAWtrust AeSign CA1 Certificate Profile Summary Table (part 1) | | | |
|--|-----------------------|---|---|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 4F B3 D1 CB | The LAWtrust AeSign CA's unique serial number. |
| | Signature Algorithm | SHA1/RSA | Algorithm to produce signatures |
| | Issuer | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd. O = LAWtrust C = ZA | Entries describing the Issuer in terms of the DN. |
| | Valid from | Not valid before date (Thursday, February 7, 2013 2:09:23 PM) | |
| | Valid to | Not valid after date (Tuesday, February 7, 2023 2:39:23 PM) | |
| | Subject | CN = LAWtrust AeSign Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd. O = LAWtrust C = ZA | Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust AeSign CA. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 cd 06 76 42 54 64 6c 9f f0 52 d3 63 d9 f7 ea a5 11 4e 39 64 c4 92 2b 5b 7d 9d 31 4d 70 9b a3 17 70 db 68 1f 54 20 87 12 e1 f8 72 50 5e d1 2a 0a c6 d6 5d 97 2d 8d 5d 63 45 94 f8 7c 1a 2b 12 e6 24 1d 3a 32 cb 35 a1 6b f4 38 0a f2 83 15 41 a2 f1 74 c6 39 b4 17 8c 25 e6 96 d1 6d ef 49 68 b6 00 ac c6 fc b4 32 3b 66 98 b8 15 d4 90 3f 29 21 e6 59 5e 6a 8f f8 e9 71 68 5b ac 26 e1 d1 22 e0 48 f1 b5 2d 18 f4 da 19 0b e7 bc fc 87 9f 0d 05 ef e8 f4 e1 65 a4 24 4f 6f 1a b2 3f 61 42 f2 0c 14 16 52 0c 9f 66 aa 64 b6 e8 9a 4c 0b 15 53 d4 d0 55 fa de ab fe 95 d7 20 c1 98 df dd 07 2e 4c f2 02 69 15 cd dd 57 e7 dd 56 19 16 ba ab 53 6b 45 5d 18 e2 8e 51 ae f1 12 df 3a d9 fb 0e 2a da 35 4b b2 9b e3 ac 53 d7 f6 27 7f c9 cb 4a c9 96 b6 44 07 36 90 41 02 cb 15 f8 eb fb 68 5e 53 1f 02 03 01 00 01 | The public key of the LAWtrust AeSign CA1. |
| | Key Usage | Certificate Signing, Off-line CRL Signing, CRL Signing (06) | Specifies practical usage of certificate |
| Private key usage period | N/A – full life of CA | Dates within which the private key is valid. | |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust AeSign CA1 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|------------------------|-------------------------|---|---|
| Certificate Extensions | Certificate Policies | <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 | <p>[1] CRL Distribution Point Full Name: http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl</p> <p>[2] CRL Distribution Point Full Directory Name: CN=CRL1 CN=LAWtrust Root Certification Authority 2048 OU=LAW Trusted Third Party Services PTY Ltd. O=LAWtrust C=ZA</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<Number>, 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> |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust AeSign CA1 Certificate Profile Summary Table (part 3)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|---|--|
| Certificate Extensions | 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 key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number. |
| | Subject Key Identifier | KeyID=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 |
| | Entrust Version Info | Entrust Authority Security Manager Version=V8.1 Key Update Allowed=Yes Certificate Category=Web | Information specifying the Version of the Entrust Security Manager Software |
| Certification Hierarchy | Certification Path | LAWtrust Root Certification Authority 2048 ↳ LAWtrust AeSign Certification Authority | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |


| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


7.4 LAWtrust AeSign CA2

| LAWtrust AeSign CA2 Certificate Profile Summary Table (part 1) | | | |
|--|--------------------------|--|---|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 4f b3 d4 60 | The LAWtrust AeSign CA2's unique serial number. |
| | Signature Algorithm | sha256RSA | Algorithm to produce signatures |
| | Issuer | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd. O = LAWtrust C = ZA | Entries describing the Issuer in terms of the DN. |
| | Valid from | Not valid before date (08 March 2017 01:05:59 PM) | |
| | Valid to | Not valid after date (08 March 2027 01:35:59 PM) | |
| | Subject | CN = LAWtrust AeSign CA02 OU = AeSign O = LAWtrust E = info@lawtrust.co.za L = Centurion S = Gauteng C = ZA | Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust AeSign CA. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 ad 2a bc 3b f5 5d 3d 55 e5 97 07 47 75 8a ee ad 09 d5 8c 02 f8 81 c7 98 a2 85 39 a6 bc 4d 31 f0 51 de 0a fa f4 e6 c9 64 45 5c 04 8f d6 bf f4 96 5f e2 01 11 f7 1b 15 9c e0 cc 1d 09 7c b4 d7 cc c5 3e 4c ad 1f a6 be e8 c8 5e 57 f2 98 30 b3 bd 49 5a 82 42 65 cd d8 1e b0 e3 c0 45 11 87 92 e5 62 c7 63 4a 4f 7e 96 87 49 9d ae f1 ae e8 2f 89 c3 4e b4 c1 c5 66 e7 49 24 af ba 96 56 62 4c ea 1b ed 21 a2 9e b7 f6 c9 97 1f fa d3 a5 19 6d f0 ac 77 97 ab 0d b7 07 6f 07 db 90 8c e7 75 27 87 1c d7 a3 c0 a9 fe 47 af 3b 73 be 38 6e ba f8 87 ab 6e ba c6 46 b0 fd c3 1a e7 83 28 c5 38 ec 1a 54 3b ae 08 fb f5 a0 3b 29 d5 6f e8 dc e5 45 41 77 a5 1f 00 2d 14 d5 6d 61 fe e5 17 97 63 90 95 2f 65 d4 bb 56 1f 9a 9f d1 8d 4f 2e 9d 84 be f4 7c 65 0e 5a 03 35 12 e3 00 c5 b3 8e 72 b2 76 bb 02 03 01 00 01 | The public key of the LAWtrust AeSign CA2. |
| | Key Usage | Certificate Signing, Off-line CRL Signing, CRL Signing (06) | Specifies practical usage of certificate |
| | Private key usage period | N/A – full life of CA | Dates within which the private key is valid. |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust AeSign CA2 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|--|--|
| Certificate Extensions | CRL Distribution Points | <p>[1] CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=LAWtrust Root 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_ca_root_za_crlfile.crl</p> <p>URL=ldap://ROOTCA1/cn=LAWtrust%20Root%20Certification%20Authority%202048,ou=LAW%20Trusted%20Third%20Party%20Services%20PTY%20Ltd.,o=LAWtrust,c=ZA?certificateRevocationList?base</p> <p>URL=file://\rootca1\CRL\lawtrust_ca_root_za_crlfile.crl</p> | <p>The LAWtrust AeSign CA2 will issue CRLs and make them available via 1] http at http://aesigncrl.lawtrust.co.za.</p> <p>The CA will issue at least one crl publication by the end of each business day.</p> |
| | Authority Key Identifier | KeyID= 5c de 3a 33 34 49 64 c4 92 31 7c 55 5e f5 f2 3b 4f ee c3 1d | The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number. |
| | Subject Key Identifier | KeyID= 11 99 14 94 a5 d1 59 93 61 71 8c a5 ae 23 0c 48 c1 fc bb 1b | 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=CA Path Length Constraint=None | Constraints description |
| Certification Hierarchy | Certification Path | LAWtrust Root Certification Authority 2048  LAWtrust AeSign Certification Authority | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

7.5 LAWtrust AATL CA1

| LAWtrust AATL CA1 Certificate Profile Summary Table (part 1) | | | |
|--|---------------------|--|--|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 4fb3d4b1 | The LAWtrust AATL CA1's unique serial number. |
| | Signature Algorithm | sha256RSA | Algorithm to produce signatures |
| | Issuer | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd. O = LAWtrust C = ZA | Entries describing the Issuer in terms of the DN. |
| | Valid from | Wednesday, 15 August 2018 11:43:44 AM | |
| | Valid to | Tuesday, 15 August 2028 12:13:44 PM | |
| | Subject | CN = LAWtrust AATL CA01 OU = organizationidentifier(4570229049) O = LAW Trusted Third Party Services PTY Ltd. E = info@lawtrust.co.za L = Centurion S = Gauteng C = ZA | Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust AATL CA1. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 8f bc b3 b5 05 44 eb b1 92 33 2d 3b dc af 5d 23 7c d8 a7 0b b4 b1 a4 fe 9a 0f 80 da bc c4 56 0e a9 02 33 d4 ce 7e 80 ff 3d 62 48 55 cc d0 6b 27 68 c9 ff 66 99 26 0c e2 5b 41 72 64 3d 6d 04 c7 51 18 58 94 4b 53 31 55 e0 fb de 69 7e 83 3a bb ef 47 68 79 30 04 92 cc 63 70 6c 0e 71 d0 2f 2d 5f e4 39 59 1c ff ae 71 9a 62 36 35 1c ba 58 dc a5 67 71 61 7e 0c ae 9e 69 5a 60 b9 c6 55 4a 34 ab 09 0f 61 8e 54 be a1 14 86 db 17 a2 2c 32 41 58 62 8c 28 7e 88 7c 7f 46 b2 f7 8a 3b 0b 79 da f7 a3 50 00 5c 52 81 28 ab a5 11 ac 0c 01 33 e0 10 65 2f 89 c2 f0 1b a4 bd 25 ad b8 10 10 52 b5 d2 55 c0 26 36 7d 3c 63 12 98 63 b4 07 ec 88 ef 56 40 ff be c5 75 72 3e d7 9a 59 60 6e b5 0f f0 b4 00 96 51 8a c1 dc 20 42 b5 67 7b e9 d3 31 45 94 14 66 ba 17 d3 12 d3 dc a2 9d eb 19 bc f0 e5 02 03 01 00 01 | The public key of the LAWtrust AATL CA1. |
| | Key Usage | Certificate Signing, Off-line CRL Signing, CRL Signing (06) | Specifies practical usage of certificate |
| Private key usage period | | Dates within which the private key is valid. | |


| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

LAWtrust AATL CA1 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|------------------------|-------------------------|--|--|
| Certificate Extensions | Certificate Policy | <p>[1]Certificate Policy: Policy Identifier=2.16.840.1.114028.10.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.lawtrust.co.za/repository [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=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 | <p>[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=LAWtrust Root 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_ca_root_za_crlfile.crl URL=ldap://ROOTCA1/cn=LAWtrust Root Certification Authority 2048,ou=LAW Trusted Third Party Services PTY Ltd.,o=LAWtrust,c=ZA?certificateRevocationList?base (ldap://ROOTCA1/cn=LAWtrust%20Root%20Certification%20Authority%202048,ou=LAW%20Trusted%20Third%20Party%20Services%20PTY%20Ltd.,o=LAWtrust,c=ZA?certificateRevocationList?base) URL=file://\rootca1\CRL\lawtrust_ca_root_za_crlfile.crl</p> | <p>The LAWtrust AATL CA1 will issue CRLs and make them available via:</p> <p>URL=http://crl.lawtrust.co.za/crl/LT_AATL_CA01.crl</p> |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust AATL CA1 Certificate Profile Summary Table (part 3)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|---|--|
| Certificate Extensions | Authority Key Identifier | KeyID=5cde3a33344964c492317c555ef5f23b4feec31d | The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a key Identifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number. |
| | Subject Key Identifier | KeyID=86 e0 e6 4d bf f1 db 14 f8 02 ac 65 61 9e 65 2e 77 3c aa 20 | 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=CA Path Length Constraint=None | Constraints description |
| Certification Hierarchy | Certification Path | LAWtrust Root Certification Authority 2048  LAWtrust AeSign Certification Authority | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


7.6 LAWtrust LTCA2048

| LAWtrust LTCA2048 Certificate Profile Summary Table (part 1) | | | |
|--|-----------------------|---|--|
| Field Type | Field Name | Value | Explanation |
| X509 fields | Version | V3 | As specified in X509 Version 3. |
| | Serial Number | 4F B3 D1 E8 | The LAWtrust Certification Authority 2048's unique serial number. |
| | Signature Algorithm | SHA1/RSA | Algorithm to produce signatures |
| | Issuer | CN = LAWtrust Root Certification Authority 2048 OU = LAW Trusted Third Party Services PTY Ltd O = LAWtrust C = ZA | Entries describing the Issuer in terms of the DN. |
| | Valid from | Not valid before date (Monday, September 2, 2013 10:21:51 AM) | |
| | Valid to | Not valid after date (Saturday, September 2, 2023 10:51:51 AM) | |
| | Subject | CN = LAWtrust Certification Authority 2048 O = LAWtrust C = ZA | Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust Certification Authority 2048. |
| | Public Key | 30 82 01 0a 02 82 01 01 00 d3 6f 33 81 03 3d f5 89 7d 03 fe 88 c8 e1 7f bb ba 6c 07 db b4 2f 1d 99 92 85 43 04 fa 26 78 70 b4 ca dd ad ac fa 50 bb 56 4f 3b 24 6d 84 ca 8d 03 20 d3 3f 12 60 e5 35 ca 8f ae 2f d8 ca 4a 83 b2 9b db d7 a6 41 dc 17 8e 6b b9 28 38 ed ba 11 c4 a9 da 75 85 f8 8a 1f b5 60 4f 37 0b ce 2c c3 4d 51 18 5c 40 91 93 d6 8a 4b b8 77 28 52 5d df b9 d0 7b 2d e2 5c be f4 2e 6d ac 5a 25 34 17 61 1f 33 1d 8d f8 7f 95 e1 92 a3 24 6e 43 cd 69 c6 e5 8f 57 2d 9c 95 0a 6a 3d 22 87 0f 2a 8d af 93 9c b2 15 a6 5c f2 cb 1c 54 a5 be 76 fc 20 09 13 67 e6 01 27 aa 65 6a 38 6c b4 1b 67 0d 4c 5e 51 8b be 06 a6 8e 53 c6 bb ba 1a 85 92 f6 90 dc 0f 29 3a 32 77 43 41 a5 f4 42 f9 6d 13 4f 75 8f e4 f2 e4 2f e2 6f 65 dd 0c c7 79 0f 84 b6 9b 83 c6 a6 4b a5 d5 91 ac 37 24 b5 a9 bf 17 e4 51 df 37 02 03 01 00 01 | The public key of the LAWtrust Certification Authority 2048 |
| | Key Usage | Certificate Signing, Off-line CRL Signing, CRL Signing (06) | Specifies practical usage of certificate |
| Private key usage period | N/A – full life of CA | Dates within which the private key is valid. | |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust LTCA2048 Certificate Profile Summary Table (part 2)

| Field Type | Field Name | Value | Explanation |
|------------------------|-------------------------|---|--|
| Certificate Extensions | Certificate Policy | <p>[1]Certificate Policy:</p> <p>Policy Identifier=2.16.840.1.114028.10.2.1</p> <p>[1,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p>https://www.lawtrust.co.za/repository</p> <p>[1,2]Policy Qualifier Info:</p> <p>Policy Qualifier Id=User Notice</p> <p>Qualifier:</p> <p>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 | <p>[1]CRL Distribution Point</p> <p>Full Name: http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crlfile.crl</p> <p>[2]CRL Distribution Point</p> <p>Full Directory Name: CN=CRL1</p> <p>Address: CN=LAWtrust Root Certification Authority 2048</p> <p>OU=LAW Trusted Third Party Services PTY Ltd.</p> <p>O=LAWtrust</p> <p>C=ZA</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<Number>,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> |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


LAWtrust LTCA2048 Certificate Profile Summary Table (part 3)

| Field Type | Field Name | Value | Explanation |
|-------------------------|--------------------------|---|---|
| Certificate Extensions | Authority Key Identifier | KeyID=5c de 3a 33 34 49 64 c4 92 31 7c 55 5e f5 f2 3b 4f ee c3 1d | 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=93 da eb 6d 26 34 ac 2e af 3d 55 74 1e 4c 82 c1 d8 a8 da cb | 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 |
| | Entrust Version Info | Entrust Authority Security Manager Version=V8.1 Key Update Allowed=Yes Certificate Category=Web | Information specifying the Version of the Entrust Security Manager Software |
| Certification Hierarchy | Certification Path | LAWtrust Root Certification Authority 2048 ↳ LAWtrust Certification Authority 2048 | An ordered sequence of certificates of entities which, together with the public key of an initial entity in the path, can be processed to obtain the public key of the final entity in the path |


| | | |
|---|-------------------------|--|
|  <p>information security solutions company</p> <p>www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

8. APPENDIX B (Definitions)


| Term | Definition |
|-------------------------|--|
| applicant | An entity making an application for a digital certificate. |
| Asymmetric cryptography | Asymmetric cryptography or public Key cryptography is cryptography in which a pair of keys issued to a subscriber and the keys are used to encrypt and or decrypt messages to achieve authenticity and confidentiality. An applicant applies for a digital certificate, if successful a key pair is generated and a certificate signing request is sent to a certificate Authority which then signs the public key and returns a public key certificate to the applicant. The public key and its corresponding private key are uniquely linked mathematically. |
| audit trail files | Secured audit log/trail files are stored on the CA server and can only be viewed by authorised personnel logged into the administration interface. |
| Authentication | Authentication is a mechanism to validate the identity of a user and or a computing device requesting permission to access computing resources or technology services supporting business processes. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

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

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

| Term | Definition |
|----------------------------------|--|
| certificate policy | A named set of rules that indicate the applicability of a digital certificate to a particular community and or class of application with common security requirements. The practices required to give effect to the rules set out in the certificate policy are set out in the certification practice statement. |
| certification practice statement | In order to comply with the rules set out in the certificate policy, the CPS details the practices that a certificate authority needs to employ when issuing, managing, revoking, renewing, and providing access to digital certificates, and further includes the terms and conditions under which the certificate authority makes such services available. |
| CP | See definition of certificate policy. |
| CPS | See definition of certification practice statement. |
| Chained | A Certificate Chain linking the chain of trust from the highest level of trust, that being the Root CA, any subordinate CA's and or Issuing CA's. |
| cryptography | Cryptography is about message secrecy, and is a main component in information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, not usually the existence of such messages. |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|-----------------------|--|
| cryptography services | A service provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of a digital certificate/digital signature scheme for the purpose of ensuring (i) that data or data messages can be accessed or can be put into an intelligible form only by certain persons, (ii) that the authenticity or integrity of such data or data message is capable of being ascertained, (iii) the integrity of the data or data message, or (iv) that the source of the data or data message can be correctly ascertained. |
| data | Electronic representations of information in any form. |
| data message | Data generated, sent, received or stored by electronic means. |
| digital certificate | A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number. |
| digital signature | A transformation of a data message using an asymmetric cryptosystem such that a person having the initial data message and the signer's public key can determine whether: (i) the transformation was created using the private key that corresponds to the subscriber's public key; and (ii) the message has been altered since the transformation was made. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|------------------------------|--|
| digital signature validation | <p>In conjunction with the public key component of the correct public/private key pair, the signature of a data object can be verified by:</p> <ol style="list-style-type: none"> 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid. |
| digitally sign | <p>The act of generating a digital signature for a data message, which is created by:</p> <ol style="list-style-type: none"> 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. <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 is called the signature and is bound to the data message according to an application specific mechanism.</p> |
| ECT Act 2002 | See definition of Electronic Communications and Transaction Act 2002 |
| electronic communication | Communication by means of data messages. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|---|---|
| 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. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|-------------------|--|
| Identity Document | <p>An identity document is used to verify aspects of a person's identity. Recognized identity documents for natural persons are;</p> <ol style="list-style-type: none"> 1. For South African citizens applying from within or outside of the South African Border; <ol style="list-style-type: none"> a. The applicant should be a current and valid citizen of South Africa. (Presence of ID document is sufficient) b. A valid and original "Green" Identity document or National ID Card issued by the South African Department of Home Affairs c. A valid and original Passport issued by the South African Department of Home Affairs d. A valid and original temporary identity document issued by the South African Department of Home Affairs. 2. For non-South African Nationals, applying from any location outside of the applicant's stated country of citizenship. <ol style="list-style-type: none"> a. The applicant should be a current and valid citizen of stated country of citizenship. (Presence of ID document is sufficient) b. Passport issued by the applicant's stated country of citizenship's, authorized government body responsible for issuing passports to citizens of the stated country, or <ol style="list-style-type: none"> 1. identity document issued from the authorized government body responsible for issuing identity documents to citizens of the stated country. |
| integrity | Integrity is a cryptography service that ensures that modifications to data are detectable. |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|-------------------------------------|---|
| key pair | Two mathematically related cryptographic keys, referred to as a private key and a public key, having the properties that (i) one key (the public key) can encrypt a message which only the other key (the private key) can decrypt, and (ii) even knowing the one key (the public key), it is computationally infeasible to discover the other key (the private key). |
| LAWtrust Root CA | See also the definition of certification authority. The Root certification authorities managed by LAWtrust including the LAWtrust Root Certification Authority 2048 and the LAWtrust Root Certification Authority 2 (4096) |
| LAWtrust Subordinate CA Certificate | See definition of digital certificate. 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, |

| | | |
|--|-------------------------|--|
|  www.lawtrust.co.za | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |


| Term | Definition |
|---------------------------|---|
| non-repudiation | The ability to prevent a party from refusing to fulfil an obligation or denying the truth or validity of an electronic communication facilitated by appropriate use of the LAWtrust Services. |
| OCSP | Online Certificate Status Protocol is an Internet protocol, employed to ascertain the revocation status of an X.509 digital certificate. An alternative to CRL based checking. |
| OCSP Responder | An online service hosted by Lawtrust and connected to Lawtrust repositories in order to process OCSP certificate revocation checks. |
| private key | The key of a key pair used to create a digital signature and is required to be kept secret. |
| public key | The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed. |
| Public key cryptography | Public key cryptography is about using mathematically related keys, a public key and a private key, in order to implement a digital certificate /digital signature scheme, also known as an asymmetric crypto system. |
| PKI | See definition of public key infrastructure. |
| public key infrastructure | The structure of hardware, software, people, processes and policies that collectively support the implementation and operation of a certificate-based public key cryptography scheme. |
| RA | See definition of registration authority. |
| registration authority | An entity that: (i) receives certificate applications, and (ii) validates information supplied in support of a certificate application, (iii) requests a certificate authority to issue a certificate containing the information as validated by the registration authority, and (iv) requests a certificate authority to revoke certificates issued; |

| | | |
|---|-------------------------|--|
|  <p>information security solutions company</p> <p>www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

| Term | Definition |
|-------------------------|--|
| 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 |
| signature | Any mark made by a person that evidence's that person's intention to bind himself/herself to the contents of a document to which that mark has been appended. Depending on the circumstances, this could be a handwritten signature or a digital signature. |
| subscriber | an applicant whose Certificate Application has been approved, and has been issued a certificate, and who is the subject named or otherwise identified in the certificate, controls the private key that corresponds to the public key listed in that certificate, and is the individual to whom digitally signed data messages verified by reference to such certificate are to be attributed. |
| 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. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

| Term | Definition |
|--------------|---|
| Verification | <p>Verification is the act of checking that information is accurate. It is used in the following manor</p> <ul style="list-style-type: none"> a) At registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity; b) During use, the act of comparing electronically submitted identity and credentials with stored values to prove identity. c) Relying Party will check the certificates used as per the relying Party Agreement. |

| | | |
|--|-------------------------|--|
|  <p>information security solutions company www.lawtrust.co.za</p> | Classification | LEVEL 1: PUBLIC INFORMATION |
| | Reference | LT_ISP_IS_CP_V012_2019-03-08 |
| | Location | https://www.lawtrust.co.za/repository |
| | Version | V012_2019-03-08 |
| | Policy Authority | LAWtrust PA |

9. SIGN OFF ACCEPTANCE

| | |
|-------------------|---------------------------|
| Name: | Katekani Hlabathi |
| Authority: | Policy Authority |
| Title: | Chief Information Officer |
| Date: | 2019-03-08 |
| Signature: | |