 <p>information security solutions company</p> <p>www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

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.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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, Added approval Signature on last page, Updated Certificate profiles, deleted CA1 and added CA2	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, table overlap)	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

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

V012 2019-03-08	2019-03-08	E Oosthuizen	Review and Housekeeping items	Expired
V013 2020-02-13	2020-02-13	K Hlabathi	Annual review. Update AeSign CA01 certificate details after rekey	Expired
V014 2020-08-25	2020-08-25	M De Waal K Hlabathi	Updated with Root CA2 information	Expired
V015 2020-10-30	2020-11-25	K Hlabathi	Updated with new Issuing CA Profile information after the Key Ceremony	Operational

Document references

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

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

 <p>information security solutions company</p> <p>www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

TABLE OF CONTENTS

1. PURPOSE	9
2. SCOPE.....	10
3. POLICY STATEMENT.....	11
3.1 LAWtrust CPS	11
3.2 Digital certificate intended usage	11
3.3 Subscriber identification and authentication	11
3.4 Publication of a digital certificate status	12
3.5 Subscriber private key protection	12
3.6 Issuer private key protection.....	12
3.7 X509 V3 Mandatory Field requirements	12
4. OBLIGATIONS AND LIABILITIES	13
4.1 Issuer.....	13
4.2 Relying Party	13
5. SECURITY MANAGEMENT	14
5.1 Policy Structure.....	14
5.2 Policy Administration.....	14
6. GOVERNING LAW.....	15
7. APPENDIX A [Digital Certificate Specification]	16

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.1 LAWtrust Root CA 2048 Certificate Profile Summary Table (part 1).....17

7.2 LAWtrust Root CA 2048 Certificate Profile Summary Table (part 2).....19

7.3 LAWtrust Root CA2 (4096) Certificate Profile Summary Table (part 1)21

7.4 LAWtrust Root CA2 (4096) Certificate Profile Summary Table (part 2)24

7.5 LAWtrust2048 CA2 Certificate Profile Summary Table (part 1)25

7.6 LAWtrust2048 CA2 Certificate Profile Summary Table (part 2)28

7.7 LAWtrust2048 CA2 Certificate Profile Summary Table (part 3)29

7.8 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 1).....29

7.9 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 2).....32

7.10 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 3).....33

7.11 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 1).....34

7.12 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 2).....37

7.13 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 3).....38

7.14 LAWtrust (AATL) Certificate Profile Summary Table (part 1)38

7.15 LAWtrust (AATL) Certificate Profile Summary Table (part 2)41


7.16 LAWtrust (AATL) Certificate Profile Summary Table (part 3)43

7.17 LAWtrust Signing CA01 Certificate Profile Summary Table (part 1)44

7.18 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)46

7.19 LAWtrust Signing CA01 Certificate Profile Summary Table (part 3)48

7.20 LAWtrust Auth CA01 Certificate Profile Summary Table (part 1)49


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.21 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)51

7.22 LAWtrust Signing CA01 Certificate Profile Summary Table (part 3)52

8. APPENDIX B (Definitions).....53

9. SIGN OFF ACCEPTANCE.....64

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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 manages and operates two PKI hierarchies offering certification services from the LAWtrust managed issuing CA’s to their clients.


1. a LAWtrust Hierarchy consisting of two Root CAs and all issuing CA’s signed into those roots 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 2048”, “LAWtrust Root CA2 (4096)”, “LAWtrust AeSign CA”, “LAWtrust AeSign CA2”, “LAWtrust Auth CA1”, “LAWtrust Signing CA01” and the “Entrust chained CA, LAWtrust 2048 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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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.

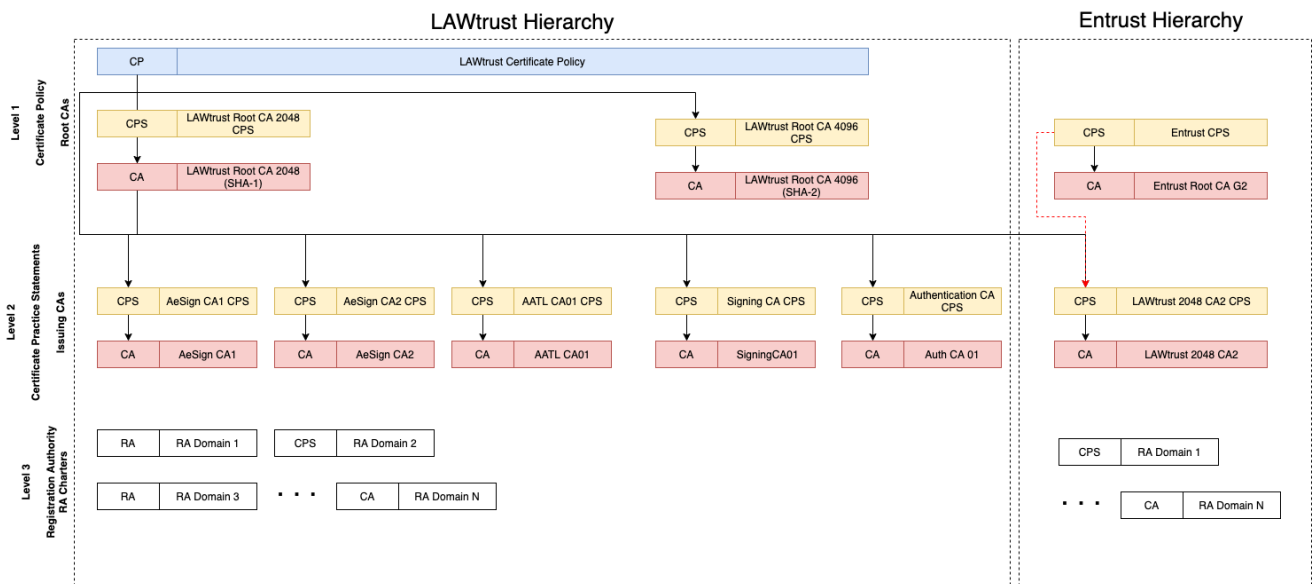



Figure 1: Certification Authorities and Governance documents of LAWtrust PKI

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. Each Root CA has a dedicated CPS and each issuing CA chained into the root CA has their own dedicated CPS.

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

 <small>information security solutions company</small> www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7. APPENDIX A [Digital Certificate Specification]


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.1 LAWtrust Root CA 2048 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	4F B3 D0 EE	The LAWtrust Root CA 2048 unique serial number.
	Signature Algorithm	SHA1/RSA		Algorithm to produce signatures
	Issuer	DN	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	Date, Time	Not valid before date (Wednesday, May 16, 2012 5:40:18 PM)	
	Valid to	Date, Time	Not valid after date (Sunday, May 16, 2032 6:10:18 PM)	
	Subject	DN	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.


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

	Public Key	RSA 2048 bit keypair	<pre> 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 </pre>	The public Key unique to the LAWtrust Root CA 2048.
	Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usages of the LAWtrust Root CA certificate
	Private key usage period	Not valid before: date Not valid after: date	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

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

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	CRL Distribution Points	URL	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crfile.crl</p> <p>[2]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>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 9f 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.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.3 LAWtrust Root CA2 (4096) Certificate Profile Summary Table (part 1)


Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	55 1a 6c 40	The LAWtrust Root CA2 (4096) unique serial number.
	Signature Algorithm	SHA256/RSA		Algorithm to produce signatures
	Issuer	DN	CN = LAWtrust Root CA2 (4096) O = LAWtrust C = ZA	Entries describing the Issuer in terms of the DN.
	Valid from	Date, Time	Not valid before date (Tuesday, 31 March 2015 11:30:17AM)	
	Valid to	Date, Time	Not valid after date (Friday, 31 March 2045 12:00:17PM)	
	Subject	DN	CN = LAWtrust Root CA2 (4096) O = LAWtrust C = ZA	Subject details of the Root CA certificate. This uniquely identifies the LAWtrust Root CA2 (4096).

Classification	LEVEL 1: PUBLIC INFORMATION
Reference	LT_ISP_IS_CP_V015_2020-10-30
Location	https://www.lawtrust.co.za/repository
Version	V015_2020-10-30
Policy Authority	LAWtrust PA

	Public Key	RSA 4096 bit keypair	<p>C6 95 2D 48 DE BD 8E 50 3A F8 37 08 ED 7A 26 7D 95 23 8D 46 DF B9 03 EE 4D 50 75 E4 DA 44 C6 1A 37 42 AC A1 51 E0 47 B3 84 57 B5 96 40 46 EE A7 72 7E F7 0A BB 98 FA 09 C2 E6 AD 4F 60 FB 11 D4 D4 78 03 82 6C 29 E5 31 83 6D 32 1A B5 DE 1B 28 F2 5E 37 81 BF AE C3 64 2A 34 BC 28 6D 52 27 4D C7 CE 6B 54 0E 81 18 4A 92 EF 8B 78 8C 44 97 31 40 4F 5A E1 0A A1 E6 DB D6 CF EB BB 8D 6C 98 03 29 3B 52 94 C2 CB 4B 69 F7 96 3B BC 03 13 EC EC 2B 6D 6E 27 D6 5B 5E 25 C2 B4 16 71 00 49 3C F1 68 C1 1B F3 90 71 D3 D5 AE 75 6B 12 0E A6 9E A1 54 0E 2F 03 0B 47 7D A4 DE 99 A1 F6 E6 38 98 EF B5 77 DF C9 AC F3 C3 06 66 28 AC B5 59 4F 0F 67 39 30 5A 54 64 02 0D E0 32 C0 48 2E 11 4B 23 7C 9C 0C 82 55 18 22 80 39 85 B4 F4 E9 B9 51 F5 72 85 53 F6 0C 52 A8 3A 53 40 D8 E6 F0 53 06 FB 5D 7D C4 12 70 1D FB 95 BE 63 F1 96 E5 96 15 BF F8 12 E3 13 F1 B4 41 AA BA 41 B9 63 B8 F0 E4 58 5E E3 D1 31 AA 49 80 90 2F 02 05 E5 63 D6 11 75 89 A3 78 8C 56 4B 4F 51 E4 FC 81 38 9A 3B 01 68 25 75 53 C3 E3 5D 26 1E 30 98 7F DC 3A AA 9C F0 6B 66 CD 27 E7 B5 A6 32 C0 F6 D7 B2 EE 8D 01 6A 53 0B D1 86 BE CC 71 BC B4 BC FA 70 AC A1 C4 AA 58 DC C7 D5 81 6E 28 8E 5B 7C D1 6B CE 0B AF C5 18 64 07 8D 80 B3 4B 85 06 E1 AE A5 FA 89 50 1D E1 54 88 46 EE 7B 74 C9 03 04 99 8F FA 4F A0 A3 DE 55 32 15 12 46 0B 49 83 D9 3D AC FF 8E 37 90 E3 C9 D4 EA 17 12 28 D1 3D DC 30 77 21 B6 36 46 12 BF 2A C7 1B 14 4C 48 11 E5 A5 AA 3D 17 68 B7 F2 FB 0D BB 72 7A 3F CB 35 25 0C 63 01 09 89 77 92 B2 6F E1 58</p>	The public Key unique to the LAWtrust Root CA2 (4096).
--	------------	-------------------------	--	---


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

			D0 C2 D6 FC C1 2A 6E 06 FC B0 0C 9B B4 28 71 C5 41 4C 29 53 97 82 0D F1 75 51 16 0D	
Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		Specifies practical usages of the LAWtrust Root CA2 certificate
Private key usage period	Not valid before: date Not valid after: date	Not before=Tuesday, 31 March 2015 11:30:17 Not after=Friday, 31 March 2045 12:00:17		Dates within which the private key is valid.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.4 LAWtrust Root CA2 (4096) Certificate Profile Summary Table (part 2)


Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	CRL Distribution Points	URL	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http:// crl.lawtrust.co.za /CRL/ lawtrust_root_ca2_(4096)_lawtrust _za_crifile.crl</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: URL= Directory Address: CN=CRL1 cn= LAWtrust Root CA2 (4096) o=LAWtrust c=ZA</p>	<p>The LAWtrust Root CA2 (4096) 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=b99e97214e8f2484967b485cb9da0d37568132e2	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=b9 9e 97 21 4e 8f 24 84 96 7b 48 5c b9 da 0d 37 56 81 32 e2	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

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

	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 (LAWtrust Root CA2 (4096))	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


7.5 LAWtrust2048 CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	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	DN	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	Date, Time	20 May 2015 05:37:57 PM	
	Valid to	Date, Time	20 May 2025 06:07:57 PM	

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.5 LAWtrust2048 CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Subject	DN	CN = LAWtrust2048 CA2 O = LAWtrust C = ZA	Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust2048 CA2.
	Public Key	RSA 2048 bit keypair	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.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.5 LAWtrust2048 CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	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 valid before: date Not valid after: date	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.6 LAWtrust2048 CA2 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	<p>[1]Certificate Policy:</p> <p>Policy Identifier=2.16.840.1.114028.10.1.8</p> <p>[1,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p>http://www.entrust.net/cps</p> <p>[2]Certificate Policy:</p> <p>Policy Identifier=2.16.840.1.114028.10.2.1</p> <p>[2,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p>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</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=http://crl.entrust.net/g2ca.crl</p>	<p>The LAWtrust2048 CA2 will issue CRLs and make them available via 1] http://2048crl.lawtrust.co.za/CRL/lawtrust2048_ca2_lawtrust_za_crlfile.crl</p>

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.7 LAWtrust2048 CA2 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	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 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=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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.8 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	1337185599	The LAWtrust AeSign CA's unique serial number.
	Signature Algorithm	SHA256/RSA		Algorithm to produce signatures
	Issuer	DN	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	Date, Time	Not valid before date (Wednesday, 15 January 2020 at 10:52:03AM)	
	Valid to	Date, Time	Not valid after date (Tuesday, 15 January 2030 at 11:22:03AM)	
	Subject	DN	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.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.8 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Public Key	RSA 2048 bit keypair	C1 D7 C5 3F 40 53 E6 D9 C5 DC 8B A0 E4 2D A8 4F D0 75 B9 55 42 75 03 99 FB 07 41 1F 8C 21 F5 05 BE 19 6D 29 E6 58 62 41 00 EC ED 47 4A FC 14 66 33 2B F5 F2 E4 AB E6 3E D3 8D 85 B0 4B 76 14 43 76 A1 12 5F 31 39 6C 6F 94 80 8E 9C 94 84 DC DC 01 3E 9E E8 0D 53 F3 C7 DB F6 58 70 2A 05 13 E1 72 A0 18 C4 0B 8B 2E 5E 61 FA 24 8D 0C D9 F7 CD 2F 5D 69 EB C6 C6 7C 03 C4 D9 39 71 10 8C CC 7D CE 68 0C 45 52 19 82 7E 8B 85 D6 1F EB D7 B2 EE 40 B3 D9 B6 EF 25 87 AE E9 3E FF B8 5C CF E5 F2 8D 2B 3D 2B 52 D8 60 21 10 95 25 31 71 D5 9F 05 49 43 32 A6 0D 48 0A 87 00 BE 33 95 6F 1D 46 A0 1B 03 EC A2 47 D2 D2 CD 45 C6 EB 81 33 18 A1 F0 14 E9 9F DD 6C 7D A6 E6 EA 82 75 C9 27 FA 25 7B B1 EA 7A 62 80 95 BF E1 FC 61 E5 F4 B3 1A D1 26 13 8C 6D 67 CA 52 9A 3C 08 B8 CB FB 81 11 AA 7F	The public key of the LAWtrust AeSign CA.
	Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.9 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	<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>


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.9 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
	CRL Distribution Points	URL	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crfile.crl</p> <p>[2]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>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. <a href="ldap://hostname:389/cn=CRL<Number>, cn= LAWtrust Root Certification Authority, ou=LAW Trusted Third Party Services PTY Ltd.,o=LAWtrust,c=ZA">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>

7.10 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
	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.


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.10 LAWtrust AeSign CA1 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	Subject Key Identifier		KeyID=5D 2A 63 D0 89 35 C6 84 A1 B1 9A 74 C4 9A 18 C3 07 09 03 EA	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


7.11 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	4f b3 d4 60	The LAWtrust AeSign CA2's unique serial number.
	Signature Algorithm	sha256RSA		Algorithm to produce signatures

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.11 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Issuer	DN	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	Date, Time	Not valid before date (08 March 2017 01:05:59 PM)	Not valid before date
	Valid to	Date, Time	Not valid after date (08 March 2027 01:35:59 PM)	Not valid after date
	Subject	DN	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.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.11 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Public Key	RSA 2048 bit keypair	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 CA.
	Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.12 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	CRL Distribution Points	URL	<p>[1]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>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>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>


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.13 LAWtrust AeSign CA2 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	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= 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 <ul style="list-style-type: none"> □ 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


7.14 LAWtrust (AATL) Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	4F B3 D1 E8	The LAWtrust Certification Authority 2048's unique serial number.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.14 LAWtrust (AATL) Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Signature Algorithm	SHA1/RSA		Algorithm to produce signatures
	Issuer	DN	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	Date, Time	Not valid before date (Monday, September 2, 2013 10:21:51 AM)	
	Valid to	Date, Time	Not valid after date (Saturday, September 2, 2023 10:51:51 AM)	
	Subject	DN	CN = LAWtrust Certification Authority 2048 O = LAWtrust C = ZA	Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust Certification Authority 2048.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.14 LAWtrust (AATL) Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Public Key	RSA 2048 bit keypair	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	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.15 LAWtrust (AATL) Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	<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>

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.15 LAWtrust (AATL) Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
	CRL Distribution Points	URL	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://aesigncrl.lawtrust.co.za/CRL/lawtrust_ca_root_za_crfile.crl</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: 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>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. <a href="ldap://hostname:389/cn=CRL<Number>,cn=LAWtrust Root Certification Authority, ou=LAW Trusted Third Party Services PTY Ltd.,o=LAWtrust,c=ZA">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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.16 LAWtrust (AATL) Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	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=CA 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 <ul style="list-style-type: none"> □ 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

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.17 LAWtrust Signing CA01 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	55 1A 6C E3	The LAWtrust Signing Certification Authority's unique serial number.
	Signature Algorithm	SHA-256/RSA		Algorithm to produce signatures
	Issuer	DN	CN = LAWtrust Root CA2 (4096) O = LAWtrust C = ZA	Entries describing the Issuer in terms of the DN.
	Valid from	Date, Time	Not valid before date (Wednesday, September 30, 2020 12:03:27 PM)	
	Valid to	Date, Time	Not valid after date (Monday, September 30, 2030 12:33:27 PM)	
	Subject	DN	CN = LAWtrust SIGNING CA01 O = LAWtrust C = ZA	Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust Signing CA01.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.17 LAWtrust Signing CA01 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
	Public Key	RSA 2048 bit keypair	E7 39 D5 20 D4 84 3D 40 B6 BA 49 96 6D 23 5F EB 01 9A DE 85 1F 8C CE F3 B3 AF 38 BB E6 97 58 A7 37 E4 E4 26 D8 CA 18 7A CE 4E 92 A2 BF 13 79 3A C3 B3 7C 57 7C B7 BF BB 7F 07 AD 08 8A 61 19 BB D6 51 26 2A 8F 50 7A 41 16 29 9C FD 8B D7 52 DA A4 DC FD C7 61 84 99 FA 71 05 5C 75 2C 1E 3B AB D6 A8 C0 6C 1D 5B C3 BB 09 31 7E 7C 07 AF 81 8F F4 1B 06 8D 78 E3 38 E9 B5 55 9E 82 DF FB 0F 71 03 8D 4C 7A 76 0C 63 42 4C 68 00 10 2A 94 3C 44 F1 C2 5C 7E 89 14 CD FD C7 CA 8D E3 82 29 67 F7 AD 38 B9 6E 6E 19 59 41 66 83 16 28 51 38 52 A3 56 F6 C5 0C 85 C5 DF 36 9C CD 6E E5 DC 2F A1 F6 62 46 10 D7 FE 28 FE A3 D2 E0 15 43 97 F2 AB 5E B2 65 DB CF 8A 67 E2 28 89 D2 29 1D AF 23 FB 3B BD C3 72 49 9F CD 22 86 D0 6F A0 80 8A 11 75 58 16 4D B8 A0 C7 94 4E AC F4 73 EB CC C5 5E 35 F1 69 D3 1E 01 57 99 86 AA 63 7D 97 87 45 4E B6 65 8D BE C2 D3 4C 69 8F 5C 52 7D 5B 77 8B 90 E2 E3 CB DA D3 38 52 9C 8B 70 3A A7 54 E4 2B 19 AF B2 D0 EE 92 49 AA 40 7A 14 B0 B8 58 66 6E 84 AC 25 9C D1 2F 5D C4 0D 7E 80 43 31 AC AE A2 E1 2B 84 D0 69 9D 06 F7 67 F5 FD C0 44 3D 4C 6D 1E 4F 89 84 97 9A 3E 17 75 80 A6 5B 41 7B 43 3D 49 06 2E 4B 3B 1E 0F FB 36 65 7B 6F 35 4A F9 EE 14 95 AD 47 80 44 8E 5E 86 E8 73 3E 4C 84 D2 04 C9 27 0E 83 3A 86 FA F2 C2 96 71 FB 49 32 CC 0A	The public key of the LAWtrust Signing CA01.


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.17 LAWtrust Signing CA01 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
			DD EF 06 02 12 C3 86 1D ED 22 AA 9F B3 CF 93 CA CD 5D 17 7C 37 A8 E7 4E D5 BB CD 5E 94 7A C9 73 E7 E2 3E 33 37 01 F5 63 1F CC 9B 13 30 B6 A7 91 B7 C0 6B 26 DF B0 DA 38 BD DE 7C E6 0A BE BA 72 DD 38 5C 52 BE 11 E1 9A 4B B3 D7 A2 97 0B 97 17 90 30 A3 D4 03 21 C2 BB B8 9C 8E E9 32 93 47 16 0B 2E 05	
	Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	N/A – full life of CA	Dates within which the private key is valid.


7.18 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.54383.1.3 [1,1]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

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.18 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
	CRL Distribution Points	URL	[1]CRL Distribution Point Name: Full Name: URL= http:// crl.lawtrust.co.za/CRL/lawtrust_ca_root_za_(4096)_lawtrust_za_crfile.crl	<p>The location of the CRL file where any revocation for this CA will be located</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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


7.19 LAWtrust Signing CA01 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	Authority Key Identifier		KeyID=B9 9E 97 21 4E 8F 24 84 96 7B 48 5C B9 DA 0D 37 56 81 32 E2	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=65 74 14 B3 08 F1 59 E0 7A 71 61 D1 A7 73 D5 0C E1 91 DF 7C	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(4096) □ LAWtrust SigningCA01	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.20 LAWtrust Auth CA01 Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value format	Value	Explanation
X509 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	55 1A 6C E4	The LAWtrust Auth CA's unique serial number.
	Signature Algorithm	SHA-256/RSA		Algorithm to produce signatures
	Issuer	DN	CN = LAWtrust Root CA2 (4096) O = LAWtrust C = ZA	Entries describing the Issuer in terms of the DN.
	Valid from	Date, Time	Not valid before date (Wednesday, September 30, 2020 14:56:21)	
	Valid to	Date, Time	Not valid after date (Monday, September 30, 2030 15:26:21)	
	Subject	DN	CN = LAWtrust AUTH CA01 O = LAWtrust C = ZA	Subject details of the Issuing CA certificate. This uniquely identifies the LAWtrust Signing CA01.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


	Public Key	RSA 2048 bit keypair	B8 27 96 23 0C 79 25 1B 65 3E 0C F0 42 39 85 67 81 A1 52 CA EE 16 46 19 F8 BF 8C EC 48 50 F8 CA F4 E0 E9 66 7F 2E E7 37 76 D5 4C 1B B2 1C 30 0D B4 14 18 A8 19 CF D7 41 FB C3 CE E6 63 1D AD 4C 85 61 D5 BE DC 04 55 83 B5 8E 76 7F C1 CE D1 F6 55 43 D9 8B 9F EF 07 3A 04 56 FB EC 7B 86 BD 30 E7 D3 14 31 46 2E FA F9 2D A1 1A 17 D4 76 0F 44 8D 83 84 F4 B3 7F A7 BD 0D 2B 93 CB F0 3D 28 DC D3 0D 17 6A 2B CE 26 BB 44 01 FE 83 EB 86 46 F1 8E E5 40 2C 54 7E 19 E0 DD 81 6E B4 27 FA D2 14 78 41 65 F4 52 94 6E 03 AF F8 FC F1 43 44 6A 04 DF E6 09 1F 63 97 1E 1C 92 A0 89 42 79 74 CD 66 A8 1F 1A 30 B1 BC 1B 1E 1A 8D F3 3A 49 8B 5E 40 D2 B6 40 58 A7 DE C4 87 BB 43 F2 41 4E A0 36 56 95 C2 C0 D8 B2 AE 4A 3A BD 87 21 E6 16 4C 30 62 C2 D0 28 14 2D B5 47 61 BD 7E B8 9C E5 21 B2 ED 2A 90 C0 B5 EB 93 FC 5C 84 A3 F0 84 F0 57 C0 DE D3 10 1B 18 BA D1 24 A3 62 44 51 54 8E E2 3F 86 D6 E8 93 C2 23 F4 06 A1 A0 3D AC D6 4F CE DE AA 46 5B 0A 12 6C 5E A1 05 01 73 8D BF D3 8A D3 FD F7 BB 73 27 B5 95 46 B6 31 D6 CB A7 F9 AB CE DD 7D EC 0A 76 E8 34 36 6F B3 5C 32 26 81 59 25 E1 68 97 9F F7 00 47 BA B0 E3 CB E1 B1 DC 8D 9D F2 06 BD 2F 47 EC 30 14 F7 BF 21 88 5C 61 6F A6 87 64 DF D0 43 C7 45 86 3A A2 77 5F EB 6B 00 30 1C 5A 43 45 26 53 02 EF 13 1F A3 A8 D5 D9 BF 93 3C 3C 41 7B CF 92 96 83 FC A2 1A 75 7A F3 6D 4A 9D 73 FE 73 87 81 4A 24 4F 7F 73 91 2B 35 80 F7 68 69 23 97 58 77 6A 9C 49 8D 46	The public key of the LAWtrust Signing CA01.
--	------------	-------------------------	---	---

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

			24 5C 53 4A 26 32 E1 E0 D7 9F 0C 14 54 4B 5D B0 38 46 67 D4 5A 0C E1 9A 80 39 D9 47 23 4D FE FA 8F C8 72 74 AA AB 34 AC C7 7F 0C C4 17 39 0F 7A 5E 08 6E 7C BC 13	
	Key Usage	Digital Signature Key Encipherment	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	N/A – full life of CA	Dates within which the private key is valid.

7.21 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions	Certificate Policies	URL	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.54383.1.3 [1,1]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

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.21 LAWtrust Signing CA01 Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value format	Value	Explanation
	CRL Distribution Points	URL	[1]CRL Distribution Point Name: Full Name: URL= http:// crl.lawtrust.co.za/CRL/lawtrust_ca_root_za_(4096)_lawtrust_za_crfile.crl	<p>The location of the CRL file where any revocation for this CA will be located</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>

7.22 LAWtrust Signing CA01 Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value format	Value	Explanation
	Authority Key Identifier		KeyID=B9 9E 97 21 4E 8F 24 84 96 7B 48 5C B9 DA 0D 37 56 81 32 E2	<p>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.</p>


 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

7.22 LAWtrust Signing CA01 Certificate Profile Summary Table (part 3)


Field Type	Field Name	Value format	Value	Explanation
Certificate Extensions (continued)	Subject Key Identifier		KeyID=B3 60 7D FD 4A CB 9E 9C BF 16 2E 90 79 53 97 62 BB 9D A3 E4	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(4096) □ LAWtrust SigningCA01	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

8. APPENDIX B (Definitions)


Term	Definition
applicant	An entity making an application for a digital certificate.

 www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


Term	Definition
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>Something the requester is(biometrics)</p>

 <p>information security solutions company www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


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

 <p>information security solutions company www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


Term	Definition
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.
cryptology	Cryptology is about message secrecy, and is a main component in information security and related issues, particularly, authentication, and access control. One of cryptology's primary purposes is hiding the meaning of messages, not usually the existence of such messages.
cryptology 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>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA


Term	Definition
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"> 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.
digitally sign	The act of generating a digital signature for a data message, which is created by: <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>

 <p>information security solutions company</p> <p>www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

Term	Definition
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.

 <p>information security solutions company www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	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</p> <p>www.lawtrust.co.za</p>	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_CP_V015_2020-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V015_2020-10-30
	Policy Authority	LAWtrust PA

9. SIGN OFF ACCEPTANCE

Name:	Katekani Hlabathi
Authority:	Policy Authority
Title:	Chief Information Officer
Date:	2020-10-25
Signature:	