www.lawtrust.co.za		
	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_ISP_IS_RAC_LT2048CA2_V005_2018-12-14
	Location	https://www.lawtrust.co.za/repository
	Version	V005 2018-12-14
	Policy Authority	LAWtrust PA

LAWtrust2048 CA2 Registration Authority Charter

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.

COPYRIGHT NOTICE

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V001 2015-11-01	2015-11-01	Katekani Hlabathi	Final Changes	
V002 2016-11-01	2016-11-01	Bruce Anderson	2016 Review, new format	Expired
V003 2017 03 02	2017-03-01	Bruce Anderson	Amended as per housekeeping items	Expired
V004 2017-10-23	2017-10-23	Bruce Anderson	2017 Review	Expired
V005 2018-12-14	2018-12-14	Eduard Oosthuizen	Apply new document template, 2018 Review	Published

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
6	LAWtrust mPKI Services Agreements	LAWtrust & Registration Authorities

TABLE OF CONTENTS

1. INTRODUCTION

LAWtrust specialises in application security solutions with a focus on strong authentication, non-repudiation and other cryptographic solutions. This includes SSL certificates, PKI, Card and Key Management, biometric and digital signature solutions, encryption and data security solutions.

In order to deliver on the technology solutions, LAWtrust will make increasing use of the electronic environment including the Internet and Information Systems. LAWtrust needs to provide their employees, contractors, suppliers and clients with a secure electronic environment to facilitate the exchange of information and documents, electronic communications, and a secure user community. In order to preserve high levels of confidentiality and integrity in this public medium, and to align with the regulations and provisions of the Electronic Communications and Transactions Act, LAWtrust has partnered with an internationally established standard in secure communication, namely, the Entrust Public Certification Services, to deliver on their PKI security solutions.

The terms contained in this Charter are subject to the terms and conditions contained in the LAWtrust Certification Practice Statement (CPS). Combined, this Charter and the LAWtrust CPS specify the digital certification process and provide the required trust in LAWtrust as a digital certificate issuer. All persons are required to adhere to the terms and conditions contained in the LAWtrust CPS as well as any other requirements imposed by LAWtrust that do not conflict with the LAWtrust CPS.

2. Scope

This document describes the digital certificate lifecycle processes of digital certificates issued from the LAWtrust2048 CA2 CA. It directly supports the LAWtrust2048 CA2 CPS in terms of the digital certificate lifecycle.

The LAWtrust2048 CA2 RA Charter is applicable to LAWtrust as well as to all parties taking part in the LAWtrust digital certification process. The LAWtrust Policy Authority (PA) is the final authority on this Charter and all PKI Policy matters.

The LAWtrust Operations Authority is responsible for the operational implementation and maintenance of the processes as defined within the charter document.

3. Registration Authority Appointment

LAWtrust is appointed a Registration Authority (LAWTRUST2048 CA2 RA) to:

1 Accept applications for LAWtrust Certificates.

2 Perform authentication of identities and verification of information submitted by applicants when applying for the issuance of a digital certificate by the LAWtrust2048 CA2 in terms of the provisions of this Charter, which has been approved by the LAWtrust Policy Authority.

3 Where such authentication and verification is successful, submit the request to the LAWtrust2048 CA2, in accordance with the provisions of this Charter and the LAWtrust CPS.

The LAWTRUST2048 CA2 RA is appointed exclusively for the purposes of authenticating the identity and verifying supporting and ancillary information of applicants using the services provided by LAWtrust.

4. Document Name and Publication

This document is called the LT_ISP_IS_RAC_LT2048CA2_003_2017-03-02. The latest version of the Charter may be accessed at the LAWtrust website https://www.lawtrust.co.za/repository.

5. Ownership of Charter

The LAWtrust Policy Authority is responsible for the upkeep of this Charter. Changes to this Charter are to be authorised by the LAWtrust Policy Authority.

The day to day business operations (including technical) related to certificate lifecycle would be executed by LAWtrust Operations Authority.

6. Definitions and Acronyms

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.

Term	Definition
Authentication factors	A factor of authentication refers to a mechanism used to facilitate the authentication of a user or devices requesting access to computing resources. The following factors of authentication are universally accepted; Location of the computing interface(controlled access and managed), Something the requester has(Possession of something which is validated), Something the requester knows(secret password or PIN), Something the requester is(biometrics)
Authentication scheme	Industry accepted authentication schemes include one or more factors of authentication. The choice of authentication factors and the process behind establishing credentials within each factors within the chosen scheme determine the strength of the authentication.
CA	See definition of certificate/certification authority.
certificate administrator	A trusted individual that performs certain trusted tasks (e.g. authentication) on behalf of a CA or RA. This person is usually a member of the personnel of such CA or RA.
Certificate	See definition of digital certificate.
certificate/certification authority	A legal Entity that issues, signs, manages, revokes and renews digital certificates.
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.

Term	Definition
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.
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.

Term	Definition
digital certificate	A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number.
digital signature	A transformation of a data message using an asymmetric cryptosystem such that a person having the initial data message and the signer's public key can determine whether: (i) the transformation was created using the private key that corresponds to the subscriber's public key; and (ii) the message has been altered since the transformation was made.
digital signature validation	In conjunction with the public key component of the correct public/private key pair, the signature of a data object can be verified by: 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.

Term	Definition
digitally sign	The act of generating a digital signature for a data message, which is created by: 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.
ECT Act 2002	See definition of Electronic Communications and Transaction Act 2002
electronic communication	Communication by means of data messages.
Electronic Communication and Transactions Act, No. 25 of 2002	South African Legislation that provides for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy; to promote universal access to electronic communications and transactions and the use of electronic transactions by businesses.
Email	Electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication.
End Entity	certificate subject that uses its private key for purposes other than signing certificates

Term	Definition
Entity	An individual or natural person or an entity that is registered with CIPC are examples of entities. Note that a Certification Authority, a Registration Authority or an End Entity are Entities. The term Entity excludes trusts, partnerships and sole proprietors
epf	An .epf file is an Entrust desktop security store that stores keys and certificates on a user's computer (desktop user). Allows you to encrypt and sign files.
esp	Entrust Entelligence Security Provider is an enterprise-wide desktop security platform, used to manage digital identities, specifically to generate store and backup cryptographic keys for enterprise certificates.
Identity Documents for an Entity	1. a valid search done through Companies and Intellectual Property Commission (CIPC) or other accredited CIPC search provider or a Disclosure Certificate issued by CIPC, 2. power of attorney or letter of appointment by an authorised signatory of the company, close corporation, or other Entity, authorising a specific person to apply for or otherwise deal with LAWtrust in relation to the issuing, renewal or replacement of certificates, who will also be the key holder; and 3. A copy of the identity document of any authorised key holder.
Identity documents for Natural persons	Where the subscriber is a natural person, the following documents must be used for the authentication and verification of a subscriber, during initial registration, certificate renewal, routine rekey, rekey after revocation and when processing requests for suspension or revocation, 1. Identity document or Passport for initial registration 2. Accredited certificate for Certificate renewal

Term	Definition
Identity document	An identity document is used to verify aspects of a person's identity. Recognised identity documents are; For South African citizens, 1. a valid "Green" Barcoded Identity document or Passport issued by the South African Home Affairs department 2. National Identity Smartcard 3. Temporary identity document issued by the South African Home Affairs Department 4. A valid South African Driver's license For non-South African Nationals, 1. a valid Passport issued by the person's country of origin Home Affairs department.
Integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
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.

Term	Definition
LAWtrust OA	LAWtrust Management forum responsible for the implementation of the LAWtrust Policy and Practices and the Operations of the LAWtrust PKI environment
LAWtrust PA	LAWtrust Management forum responsible for defining the LAWtrust Policy and Practices and ensuring that the Policies and Practices are adhered to.
LDAP	A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Master Services Agreement	The contract between LAWtrust and an appointed registration authority stipulating the terms and conditions for the registration authority to manage certificate lifecycle activities on behalf of the LAWtrust Root CA.
MSA	Master Services Agreement,
non-repudiation	The ability to prevent a party from refusing to fulfil an obligation or denying the truth or validity of an electronic communication facilitated by appropriate use of the LAWtrust Services.
OCSP	Online Certificate Status Protocol is an Internet protocol, employed to ascertain the revocation status of an X.509 digital certificate. An alternative to CRL based checking.
OCSP Responder	An online service hosted by LAWtrust and connected to LAWtrust repositories in order to process OCSP certificate revocation checks.

Term	Definition
Owner	Individual or group that holds or possesses the rights of and the responsibilities for an enterprise, Entity or asset. Examples: process owner, system owner, Document Owner, Information Asset owner
private key	The key of a key pair used to create a digital signature and is required to be kept secret.
public key	The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed.
Public key cryptography	Public key cryptography is about using mathematically related keys, a public key and a private key, in order to implement a digital certificate /digital signature scheme, also known as an asymmetric crypto system.
PKI	See definition of public key infrastructure.
public key infrastructure	The structure of hardware, software, people, processes and policies that collectively support the implementation and operation of a certificate-based public key cryptography scheme.
RA	See definition of registration authority.
registration authority	An Entity that: (i) receives certificate applications, and (ii) validates information supplied in support of a certificate application, (iii) requests a certificate authority to issue a certificate containing the information as validated by the registration authority, and (iv) requests a certificate authority to revoke certificates issued;
Relying Party	A person that relies on a certificate or other data that has been digitally signed.

Term	Definition
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.
Verification	Verification is the act of checking that information is accurate. It is used in the following manor a) At registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity; b) During use, the act of comparing electronically submitted identity and credentials with stored values to prove identity. c) Relying Party will check the certificates used as per the relying Party Agreement.

7. Public Key Infrastructure Configuration

7.1 Applicant and Subscriber

In this Charter an Entity or End Entity applying for a LAWtrust Certificate shall be described as an "applicant" until the application for the LAWtrust Certificate has been granted. Once a LAWtrust Certificate has been issued the Entity or End Entity to whom it has been issued shall be referred to as a "subscriber".

7.2 Domain of Use (Eligibility for Certification)

Any Entity or End Entity, can be digitally certified under the following conditions:

1. The subscriber has an existing or potential business relationship with LAWtrust.
2. The subscriber has a valid e-mail account.
3. The subscriber has a cellular phone number.
4. The subscriber is in good standing with LAWtrust.
5. The subscriber is fully aware of the responsibilities regarding the care and use of digital certificates and keys (as contained in the LAWtrust CPS, this Charter and any other LAWtrust governance policies).

7.3 Purpose of Certification

Digital certification is to be used to provide the subscribers with trusted identity credentials for, amongst other uses:

1. Secure e-mail.
2. Digital signature capability to send and receive secure e-mail to and from the Internet.
3. Authentication to LAWtrust business systems.
4. File and folder encryption.
5. Digitally sign documents or transactions.

The above will ensure authentication, authorization, privacy, message integrity and non-repudiation. The subscriber may only use the LAWtrust digital certificate for legitimate purposes.

7.4 PKI Hierarchy – CA's, RA and private keys

7.4.1 PKI trust hierarchy

Entrust.net – Secure Server Certification Authority – Entrust Root Certification Authority - G2 (RCA)

- LAWtrust2048 CA2 – Local Certification and Issuing Authority (IA)
  - LAWTRUST2048 CA2 RA – Local Registration Authority (LRA)

7.4.2 PKI root key hierarchy is as follows:

Entrust.net – Entrust Root Certification Authority - G2 – ROOT CA

- LAWtrust2048 CA2 (LAWtrust Certificates to be signed by this CA) – ISSUING CA

7.5 Certificate Type & Content

7.5.1 Certificate Type

- Web dual key-pair user certificates
- Web two key pair single usage certificates
- Enterprise dual key-pair user certificates
- Enterprise two key pair single usage certificates

7.5.2 Certificate Content (Subject Details)

- Common Name (First Name & Surname)
- Serial Number
- E-mail address
- Issuing Authority: LAWtrust2048 CA2

- Organization: LAWtrust RA
- Organization: LAWtrust
- Country: ZA

7.6 Private Key Protection

Enterprise certificates are protected with the Entrust Entelligence Security Provider as the secure key store. Access to the private key is via a password which the subscriber has knowledge of.

Web Certificates utilise the operating system Key Store. Access to the private key is via a password which the subscriber has knowledge of.

8. Digital Certificate Lifecycle Processes

8.1 Applicant Identity Verification

Enterprise Certificates: Physical verification of the applicant's approved identity document.

Web Certificates: Physical verification of the applicant's approved identity document.

8.1.1 Notifications to the Subscriber

The RA shall make commercially reasonable efforts to notify the applicant and or subscriber of certain digital certificate lifecycle events.

8.1.1.1 Notification method

Notification's to the applicant or subscriber will be performed either in person by telephone or via Email, using the eMail address documented in the application form, unless a different mechanism is specified.

8.2 Application for a LAWtrust Certificate

The LAWTRUST2048 CA2 RA shall be entitled to accept and process applications for Entities and End Entities for the issuance of a LAWtrust Certificate.

As a minimum the LAWTRUST2048 CA2 RA shall require from the End Entity or natural person applicant:

1 A duly completed and signed LAWtrust certificate application form.

2 A duly completed and signed Subscriber Agreement.

3 Copy of the applicant's approved identity document

8.3 Process of Certificate Request Verification

The LAWTRUST2048 CA2 RA appointed certificate administrator will perform the following steps to issue a certificate:

1 Receive a request, which has been authorized by the LAWtrust OA.

2 Obtain confirmation from the enrolment officer that Physical Confirmation of the applicant's identity against the user's approved identity document, has been concluded.

3 Register the subscriber and create the reference code and authorisation code on the LAWtrust2048 CA2 AdminServices portal.

4 Deliver the reference code (via email) and authorisation code (via SMS) that will enable the download of the certificate to the applicant (delivery in person or via secure courier is acceptable).

5 LAWTRUST2048 CA2 RA shall, if required by the applicant, provide telephonic assistance to the applicant in the activation of the LAWtrust Certificate.

8.4 Advising on the Outcome of the Application

If the application is refused the LAWTRUST2048 CA2 RA shall give the applicant notice of the refusal by the LAWTRUST2048 CA2 RA.

The process to notify the applicant shall follow section 8.1.1 and shall provide the reasons for the refusal.

If the application is granted, the LAWTRUST2048 CA2 RA, within 10 (ten) days of the receipt of the application will advise the applicant that the enrolment for a LAWtrust Certificate can commence.

8.5 Process of Enrolment (account creation)

8.5.1 Required fields

An electronic enrolment form will be completed and the following enrolment fields are compulsory:

1 Common name (CN) (First Name & Surname or entity name)

2 E-mail address (E)

3 Serial Number (Unique identifier)

8.5.2 Prerequisites

Once the LAWtrust Enrolment Officer has confirmed the following

1 Identity verification is successful,

2 Administrator has received the LAWtrust2048 CA2 completed signed application, including the Subscriber Agreement from the Applicant

An electronic enrolment form will be completed by the RA administrator for the Applicant on the LAWtrust2048 CA2 AdminServices portal.

8.5.3 Account creation

The LAWtrust RA Administrator will perform the following steps to create the Applicant account:

1. Log on to the LAWtrust2048 CA2 AdminServices Portal with the provided credentials.
2. Register the Applicant with the required enrolment fields and create the reference number and authorization code on the LAWtrust2048 CA2 AdminServices Portal.
3. Share Authorisation and Reference codes with the relevant party.

8.6 Certificate Issuance Process

8.6.1 Enterprise Certificate

The LAWtrust2048 CA2 RA appointed Enrolment Officer will perform the following steps onsite with the Applicant to issue the LAWtrust2048 CA2 RA Certificate:

1. Install the ESP SW on the applicant's computer
2. Click "Enroll for Entrust Digital ID"
3. Enter the Reference Number and Authorisation Code captured during the Applicant account creation process for the Applicant.
4. Ensure the LAWtrust2048 CA2 RA Certificate was successfully installed on ESP
5. Allow the Subscriber to view the LAWtrust2048 CA2 RA Certificate detail via ESP.
6. If the details on the certificate are incorrectly captured, the LAWtrust Enrollment Officer shall revoke the certificate immediately following the Revocation Process and restart the process of issuance.
7. Assist the Subscriber to test the use of the LAWtrust2048 CA2 Certificate.

8.6.2 Web Certificate

The LAWtrust2048 CA2 RA appointed Enrolment Officer will perform the following steps onsite with the Applicant to issue the LAWtrust2048 CA2 RA Certificate:

1. Change the settings on the web browser
2. Access the enrollment pages
3. Enter the Reference Number and Authorisation Code captured during the Applicant account creation process for the Applicant.
4. Ensure the LAWtrust2048 CA2 RA Certificate was successfully downloaded to the desktop
5. Allow the Subscriber to view the LAWtrust2048 CA2 RA Certificate detail via the browser

6. If the details on the certificate are incorrectly captured, the LAWtrust Enrollment Officer shall revoke the certificate immediately following the Revocation Process and restart the process of issuance.
7. Assist the Subscriber to test the use of the LAWtrust2048 CA2 Certificate.

8.7 Acceptance of Certificate

After the issuance of the LAWtrust2048 CA2 Certificate, the subscriber shall check that the content of the LAWtrust Certificate is correct.

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

8.8 Certificate Verification

- The certificate validity can be verified in the LAWtrust CRL [http://2048crl.lawtrust.co.za/CRL/lawtrust2048_ca2_lawtrust_za_crlfile.crl].
- The CRL profile will be a full CRL.
- The certificate is valid for a maximum period of up to three years from date of issue.
- The certificate validity can also be verified using ocsp on http://ocsp.lawtrust.co.za

8.9 Digital Certificate status changes

8.9.1 Rename user (change user CN)

When a Subscriber user's common name changes, e.g. a female user gets married and her surname changes, the enrolment officer is required to re-enrol the subscriber. The old certificate must be revoked and a new one issued to the Subscriber.

8.9.2 Circumstances for Revocation and Suspension Certificates

LAWtrust Certificates may be revoked under authority from the LAWtrust Chief Technology Officer under any of the following circumstances:

1. Abuse of the digital certificate by the subscriber.
2. Subscriber's request.
3. Any change in the information contained in the LAWtrust2048 CA2 Certificate issued to a Subscriber;
4. Subscriber suspected of fraudulent activity.
5. The compromise of the LAWtrust2048 CA2 private key, or if applicable, the compromise of a superior Certification Authority's private key;
6. Breach by the Subscriber of any of the terms of this LAWtrust2048 CA2 CPS or the Subscriber Agreement entered into with the Subscriber;
7. Non-payment of fees in respect of any services provided by LAWtrust or LT-RA.
8. Issue or use of the certificate not in accordance with the LAWtrust CPS.
9. If a subscriber dies and after receiving a certified copy of the subscriber's death certificate.
10. On receipt of documentary proof that a subscriber that is a legal person has been wound up, or deregistered or has ceased to exit.
11. The LAWtrust2048 CA2 or LAWtrust Root CA 2048 expires.
12. A determination by the LAWtrust2048 CA2 or a LAWtrust2048 CA2 RA that the certificate was not issued in accordance with this LAWtrust2048 CA2 CPS or the provisions of the Subscriber's Agreement entered into with the Subscriber; or
13. Any other reason that the LAWtrust2048 CA2 reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust2048 CA2 Certificate.

8.9.2.1 Certificate Revocation Processes

A request to revoke a LAWtrust Certificate may be submitted by a subscriber, the LAWTRUST2048 CA2 RA or the LAWtrust2048 CA2 if any of the above occurs.

1 The LAWTRUST2048 CA2 RA shall authenticate a request for revocation of a LAWtrust Certificate using a sub-set of the information provided by the subscriber with the certificate application.

2 Upon verification the LAWTRUST2048 CA2 RA will send a revocation request to the LAWtrust2048 CA2.

3 The LAWtrust2048 CA2 shall within 48 hours of receiving a revocation request, post the serial number of the revoked LAWtrust Certificate to the CRL in the LAWtrust repository.

4 The LAWTRUST2048 CA2 RA shall make a commercially reasonable effort to notify the subscriber as per section 8.1.1.

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

8.9.2.2 Conditions for Certificate Suspension

The LAWTRUST2048 CA2 RA may suspend a LAWtrust Certificate if:

1 The subscriber is not in good standing with the LAWTRUST2048 CA2 RA or LAWtrust2048 CA2;

2 The subscriber fails to adhere to the provisions of the LAWtrust CPS or the LAWtrust RA Charter;

3 Temporary suspension of the subscriber's role that requires the use of a LAWtrust Certificate.

The LAWTRUST2048 CA2 RA may request the LAWtrust2048 CA2 to suspend a LAWtrust Certificate without prior notice to the subscriber.

8.9.2.3 Certificate Suspension Processes

A request to suspend a LAWtrust Certificate may be submitted by a subscriber the LAWTRUST2048 CA2 RA or the LAWtrust2048 CA2 if any of the conditions listed in section 8.9.2.2 Conditions for Certificate Suspension are met.

1. The LAWTRUST2048 CA2 RA shall authenticate a request for suspension of a LAWtrust Certificate using a sub-set of the information provided by the subscriber with the certificate application.
2. Upon verification of the subscriber identity and information, the LAWTRUST2048 CA2 RA will send a suspension request to the LAWtrust2048 CA2.
3. The LAWtrust2048 CA2 shall within 24 hours of receiving a suspension request, post the serial number of the suspended LAWtrust Certificate to the CRL in the LAWtrust repository.
4. The LAWTRUST2048 CA2 RA shall notify the subscriber as per section 8.1.1, that the LAWtrust Certificate has been suspended.

Suspension of a LAWtrust Certificate shall not affect any of the subscriber's contractual obligations under the LAWtrust CPS or the Subscriber Agreement entered into by the subscriber or any Relying Party Agreements.

8.9.3 Certificate Re-Instatement process

A request to un-suspend a LAWtrust Certificate may be submitted by a subscriber, the LAWTRUST2048 CA2 RA or the LAWtrust2048 CA2 if all parties are in agreement that the reason for the initial suspension of the certificate has been resolved.

The LAWTRUST2048 CA2 RA shall authenticate a request to un-suspend a LAWtrust Certificate using a sub-set of the information provided by the subscriber with the certificate application.

Upon verification of the subscriber identity and information, the LAWTRUST2048 CA2 RA will send an un-suspend request to the LAWtrust2048 CA2.

The LAWtrust2048 CA2 shall within 24 hours of receiving an un-suspension request, remove the serial number of the suspended LAWtrust Certificate from the CRL in the LAWtrust repository.

The LAWTRUST2048 CA2 RA shall notify the subscriber as per section 8.1.1, that the LAWtrust Certificate has been un-suspended.

8.9.4 LAWtrust Certificate Renewal process

Prior to the certificate expiring, the RA will notify subscribers as per section 8.1.1, of the need to re-key prior to expiration.

The LAWtrust Certificate will be renewed on the impending expiry date of the certificate. The renewal of web certificates will be managed by the subscribers. The LAWTRUST2048 CA2 RA will issue a new reference number and a new authorisation code to the subscriber that will allow the subscriber to download a new certificate. The renewal of the enterprise (ESP) certificates will be automated and will only require the subscriber to confirm the renewal process.

During the certificate renewal the subscriber will undergo a re-key and the new public key information will be included in the new certificate. For web certificates the LAWTRUST2048 CA2 RA will confirm the identity of the subscriber applying for the renewal before the new enrolment codes are distributed.

The LAWTRUST2048 CA2 RA shall notify the subscriber as per section 8.1.1, that the LAWtrust Certificate has been renewed.

8.9.5 LAWtrust Enterprise Certificate Recovery

The LAWtrust enterprise (ESP) certificates can be used to encrypt data. When a user loses their epf file protecting the private decryption keys the user will not be able to decrypt data encrypted with a key in the epf file. In order for users to be able to recover their private decryption keys, there is a requirement for the CA to keep a copy of these keys securely in its database.

In order for a LAWtrust enterprise certificate user to recover their profile (epf) with the private decryption keys, the following process must be followed:

1 A request to recover a LAWtrust enterprise certificate may only be submitted by the subscriber if his profile (epf) has been lost, destroyed or corrupted.

2 The LAWTRUST2048 CA2 RA shall authenticate a request to recover a profile (epf) using a sub-set of the information provided by the subscriber with the certificate application.

3 Upon verification of the subscriber identity and information the LAWTRUST2048 CA2 RA will send a recover (reset) request to the LAWtrust2048 CA2.

4 The LAWTRUST2048 CA2 RA certificate administrator will deliver the reference code (via email) and authorisation code (via SMS) that will enable the recovery of the profile (epf) to the subscriber’s desktop/laptop (delivery of the codes in person or via secure courier is acceptable).

5 The LAWTRUST2048 CA2 RA shall, if required by the subscriber, provide assistance to the subscriber in using the ESP recovery wizard to recover the profile (epf) and to provide a new password to protect the profile (epf).

6 During the recovery of the profile the subscriber will undergo a re-key and the new public key information will be included in the new certificate generated for the subscriber.

8.10 Data Retention

The LAWTRUST2048 CA2 RA shall retain the following documentation securely, in conformance with the provisions of the ECT Act and regulation and in in conformance with the requirements of the LAWtrust Policy Authority, for a period of 7 (seven) years:

1 Applications for the issuing of certificates;

2 Registration and verification documents for certificates generated;

3 Certificates in a manner such that;

a. no-one, with the exception of parties authorized to do so, can make changes to the certificates;

b. it is possible to verify that the information is correct; and

4 Information related to suspended certificates;

5 Information related to expired and revoked certificates;

6 Reliable records and logs for activities that are core to the certification service provider's operations.

9. LAWTRUST2048 CA2 RA Annual Audit

The LAWTRUST2048 CA2 RA shall be audited once per calendar year for compliance with the practices and procedures set out in this Charter and the LAWtrust CPS. If the results of an audit report recommend remedial action, the LAWTRUST2048 CA2 RA shall initiate corrective action within 30 (thirty) days of receipt of such audit report.

10. References

CA Policies, Practices & Agreements:	a. LAWtrust2048 CA2 Certificate Practices Statement (https://www.lawtrust.co.za/repository). b. LAWtrust2048 CA2 Subscriber Agreement (https://www.lawtrust.co.za/repository). c. LAWtrust Relying Party Agreement (https://www.lawtrust.co.za/repository).
Legal Framework	Electronic Communications and Transactions Act of 2002 and relevant Regulations

11. Approvals

The LAWtrust2048 CA2 RA Charter must be signed by the LAWtrust PA and the LAWtrust OA.

The acceptance of this document also implies acceptance of all documents referenced in this document Signed approval forms are filed [https://www.lawtrust.co.za/repository]

12. SIGN OFF ACCEPTANCE

Name:	Katekani Hlabathi	Michael Horn
Authority:	Policy Authority	Operational Authority
Title:	Chief Information Officer	Chief Technology Officer
Date:	2018-12-14	2018-12-14
Signature:		Signed by: Michael Horn Signed at: 2018-12-19 09:16:00 + Reason: I approve this document Michael Horn