LAWtrust SIGNING CA01 Registration Authority Charter (LAWtrust SIGNING CA01 CEN-SSCD RA 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.

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V001 2020-11-02	2020-11-02	K Hlabathi	New version	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	https://www.lawtrust.co.za/repository
2	LAWtrust SIGNING CA01 CPS	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 7

2. SCOPE 7

3. Registration Authority Appointment 8

4. Document name and publication 9

5. Charter Responsibilities 10

6. Definitions and Acronyms 12

7. Public Key Infrastructure Configuration 29

7.1 Applicant and Subscriber 29

7.2 Eligibility for Certification 29

7.3 Purpose of Certification 30

7.4 PKI Hierarchy – CA's, RA and private keys 30

7.4.1 Trust hierarchy: 30

7.4.2 Root key hierarchy: 30

7.5 Certificate Type & Content 30

7.5.1 Certificate Type 30

7.5.2 Certificate Content End Entity 31

7.6 Private Key Protection 31

7.6.1 Subscriber sole control of private key 31

7.6.2 Central SSCD 32

7.6.3 Supply of SSCD's 32

7.7 Secure communication between the RA and the CA 33

8. Digital Certificate Application Processes 33

8.1 Digital Certificate Application 33

8.1.1 Application for a LAWtrust Digital Certificate 33

8.1.2 End Entity or Natural Person application 34

8.2 Digital Certificate Application Verification 34

8.2.1 Process of Certificate Request Verification 34

8.2.2 Applicant Identity Verification 35

8.3 Digital Certificate Certification 35

8.3.1 Process of Secure Key Store Issuance and Registration 35

8.3.2 LAWtrust Certificate Issuance Process 36

8.3.3 Digital Certificate Acceptance 36

8.3.4 Advising on the Outcome of the Application 37

8.4 Digital Certificate Reliance 37

8.4.1 Certificate use verification 37

8.5 Time to process certificate applications 38

8.5.1 Certificate Authority 38

8.5.2 Registration Authority 38

8.6 Proving possession of private key 38

9. Digital Certificate status changes 38

9.1 Rename user (change user CN) 38

9.1.1 Process for certificate contents changes 38

9.2 LAWtrust Certificate Revocation and Suspension 39

9.2.1 Circumstances for revocation and suspension 39

9.2.2 LAWtrust Certificate Revocation Process 40

9.3 LAWtrust Certificate Suspension 41

9.4 LAWtrust Certificate Re-Instatement 41

9.4.2 LAWtrust Certificate Re-Instatement process 42

9.5 LAWtrust Certificate Renewal 42

9.5.1 Automatic Renewal 42

9.5.2 Manual Renewal 43

9.6 LAWtrust Certificate re-key 43

9.6.1 Re-Key After Expiry 43

9.6.2 Re-Key After Revocation 44

9.6.3 Re-Key After Name Change 44

10. SCCD Lifecycle Management 44

10.1 Subscriber private key generation and storage 44

10.2 Life cycle management of the SSCD. 44

10.2.1 Central SSCD 44

10.3 LAWtrust SSCD PASSWORD Reset 45

10.4 LAWtrust Mobile Number Reset 45

11. Other responsibilities of the Error! Unknown document property name. 45

11.1 Audit trails 45

11.2 Confidentiality 46

11.3 Annual Audit 46

11.4 Other 46

12. Termination of RA Responsibilities 46

12.1 Circumstances for termination 46

12.2 Communication 47

12.3 Planning 47

12.4 Data Management 47

13. Error! Unknown document property name. Annual Audit 48

14. References 49

15. SIGN OFF ACCEPTANCE 49

1. INTRODUCTION

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

LAWtrust, in 2012, became the first company in South Africa to be accredited by the South African Accreditation Authority as a provider of authentication products and services allowing them to issue digital certificates from their managed PKI environment for the use in creating advanced electronic signatures as stipulated in the Electronic Communications and Transactions Act of 2002.

The terms contained in this Charter are subject to the terms and conditions contained in the LAWtrust Certification Practice Statement (LT_ISP_SIGNINGCA01_CEN-SSCD_CPS). Combined, this Charter and the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS specify the digital certification process for the issuance and management of LAWtrust Digital Signing signatures. All persons are required to adhere to the terms and conditions contained in the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS as well as any other requirements imposed by LAWtrust that do not conflict with the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS.

2. SCOPE

This document incorporates the LAWtrust terms and conditions of a third party wishing to incorporate LAWtrust digital lifecycle management process into their own business processes via a LAWtrust signing portal or wishing to leverage their own existing process to facilitate the LAWtrust digital lifecycle responsibilities via an API.

3. Registration Authority Appointment

LAWtrust operates a Registration Authority (LAWtrust RA) to perform identity verification and manage the digital certificate lifecycle. The terms and conditions for operating a Registration Authority issuing LAWtrust SigningCA Certificates are documented in this LAWtrust SIGNING CA01 CEN-SSCD RA Charter. The LAWtrust RA, operated by LAWtrust, is responsible for managing digital certificate lifecycles and is bound by the terms and conditions in this LAWtrust SIGNING CA01 CEN-SSCD RA Charter.

LAWtrust may appoint a third party referred to as an **RA-Agent** to perform some or all the responsibilities of the LAWtrust RA. This LAWtrust SIGNING CA01 CEN-SSCD RA Charter serves as the documented responsibilities of the LAWtrust RA and any appointed **RA Agent**. Where deviations from this LAWtrust SIGNING CA01 CEN-SSCD RA Charter exist, such deviations will be documented in a variation agreement. Detail highlighting the responsibilities between LAWtrust and any other party is included in the variation agreement and referred to as the responsibilities matrix, "RA versus RA-Agent Responsibilities Matrix".

The LAWtrust process for appointing an **Error! Unknown document property name.** includes the following:

1. LAWtrust will verify the identity of the legal entity performing the RA-Agent responsibilities using clause 3.2.2 Authentication of organisation identity"" in the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS.

2. LAWtrust and the **Error! Unknown document property name.** will agree on the RA-Agent authentication mechanisms when requesting certificate and signature services.

At a high level, the **Error! Unknown document property name.** will:

RA Capability [RA-Agent Responsibilities]		RACI			
		R	A	C	I
1.	Accept applications for LAWtrust SIGNING CA01 Certificates.	AG	LT	SU	SU
2.	Perform authentication of identities (face-to-face or equivalent) and verification of information submitted by Applicants (in compliance with the requirements of the ECT Act) when applying for the issuance of a digital certificate by the LAWtrust SIGNING CA01 in terms of the provisions of this LAWtrust SIGNING CA01 CEN-SSCD RA Charter, which has been approved by the LAWtrust Policy Authority.	AG	LT	SU	SU
3.	Where such authentication and verification is successful, submit the request to the LAWtrust SIGNING CA01, in accordance with the provisions of this LAWtrust SIGNING CA01 CEN-SSCD RA Charter and the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS.	AG	LT	SU	SU

Table 1: RA Agent Responsibilities (high-level)

4. Document name and publication

This document is the LAWtrust SIGNING CA01 Registration Authority Charter (LAWtrust SIGNING CA01 CEN-SSCD RA Charter). The latest version of the Charter may be accessed at the LAWtrust website https://www.lawtrust.co.za/repository.

5. Charter Responsibilities

RA Capability [Ownership of Charter]		RACI			
		R	A	C	I
1.	Charter Upkeep: The LAWtrust Policy Authority (PA) is responsible for the upkeep of this Charter. Changes to this Charter are proposed by RA-Agent or the Operations Authority, amended by the Policy Authority, authorised by the Security Committee and final version approved by the LAWtrust Policy Authority.	PA	PA	SC OA RA	SC OA RA
2.	Charter Implementation: The LAWtrust Operations Authority takes full responsibility for the implementation of this Charter, the associated LT_ISP_SIGNINGCA01_CEN-SSCD_CPS, and any other LAWtrust governance policies.	OA	SD	SC PA RA	SC OA RA
3.	Charter Operational responsibilities: The day to day business operations related to certificate lifecycle would be executed by LAWtrust Operations.	OA	SD	SC PA RA	SC OA RA

RA Capability [Ownership of Charter]		RACI			
		R	A	C	I
4.	Proposal for changes: The OA, the PA, the Security Committee or an RA-Agent can submit Request for changes to this Charter.	PA	PA	SC OA PA RA	SC OA PA RA
5.	Editing Charter Content: Policy Authority	PA	PA	SC OA PA RA	SC OA PA RA
6.	Reviewers: Security Committee members are responsible to review all content changes and work with the PA to agree on the content relating to changes.	SC	PA	SC OA PA RA	SC OA PA RA
7.	Final Approval: Policy Authority	PA	PA	SC OA PA RA	SC OA PA RA

Table 2: RA Capability Ownership of the Charter

6. Definitions and Acronyms

This LAWtrust RA makes use of the following defined terms, acronyms and abbreviations. The term is defined and immediately thereafter any acronyms or abbreviations derived from the term are provided. In the event of a conflict in any definitions provided or acronyms or abbreviations derived from the definitions, the LAWtrust Policy Authority shall determine the correct meaning of the provision.

Term	Definition
Accredited digital certificate	Accredited digital certificate, means a digital certificate which has been issued by a certification service provider that has had its authentication products and services accredited in terms of section 37 of the ECT Act 2002 and the accreditation was valid at the time that a digital certificate was issued. The test to check if a certificate is an accredited certificate is to 1. check that the service provider who issued the certificate is accredited by the SAAA 2. check that the certificate is valid (not revoked, not suspended, not expired).
Applicant	An Entity or a natural person who is in the process of applying for a digital certificate.
Application Programming Interface or API	An application programming interface (API) is a set of rules ('code') and specifications that software programs can follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction, like the way the user interface facilitates interaction between humans and computers.

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	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 factor within the chosen scheme determine the strength of the authentication.

Term	Definition
CA	See definition of certificate/certification authority.
CEN-SSCD Enrolment Portal	a certificate enrolment portal where a subscriber will be enrolled for a Signing account and a new LAWtrust certificate onto their Central SSCD
CEN-SSCD enrolment API	a certificate lifecycle management API where a subscriber will be enrolled for a Signing account and a new LAWtrust certificate onto their Central SSCD
Central Secure Signature Creation Device	a certificate issued by the LAWtrust AeSign CEN-SSCD CA02 and stored in accordance with the prescriptions in the ECT Act and used by a subscriber to generate advanced electronic signatures
Central SSCD Certificate	see Central Secure Signature Creation Device Certificate
Central SSCD.	The Central SSCD is created by LAWtrust on behalf of the subscriber and the SSCD is maintained on a trustworthy system. The subscriber electronic signature creation data (SCD) or private key is generated in the HSM, encrypted by the HSM with the Key Encryption Key (KEK) an exported for storage in the SSCD. When used the encrypted SCD is imported into the HSM, decrypted and used. On completion of use the SCD is deleted from the HSM. SCD generation and use is with sole control of the subscriber.
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.

Term	Definition
certificate policy	A named set of rules that indicate the applicability of a digital certificate to a particular community and or class of application with common security requirements. The practices required to give effect to the rules set out in the certificate policy are set out in the certification practice statement.
Certificate Signing Request	a certificate signing request generated and submitted to the CA.
certificate/certification authority	A legal entity that issues, signs, manages, revokes and renews digital certificates.
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.
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.
Companies and Intellectual Property Commission (CIPC)	Companies and Intellectual Property Commission (CIPC) Overview. CIPC was established by the Companies Act, 2008 (Act No. 71 of 2008) as a juristic person to function as an organ of state within the public administration, but as an institution outside the public service. The CIPC functions among others are to Registration of Companies, Co-operatives and Intellectual Property Rights (trademarks, patents, designs and copyright) and maintenance thereof;
CP	See definition of certificate policy.
CPS	See definition of certification practice statement.

Term	Definition
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.
CSR	see Certificate Signing Request
Data	Electronic representations of information in any form.
data message	Data generated, sent, received or stored by electronic means.
digital certificate or 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.

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: 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. Comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.
digitally sign	The act of generating a digital signature for a data message, which is created by: 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.
ECT Act 2002	See definition of Electronic Communications and Transaction Act 2002

Term	Definition
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.
electronic signature creation data or SCD	"electronic signature creation data" means unique data which is used by the signatory to create an electronic signature. (Also known as the Private Key)
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	An end entity is a natural person who may apply for a digital certificate. Once an end entity's application is approved, and they have been issued with a digital certificate, they are referred to as a subscriber.
Enrolment Officer	A person appointed by the LAWtrust RA or the RA-Agent to certain duties such as perform identity verification and information verification involved in the digital lifecycle management process.
Entity	An entity that is registered with CIPC are examples of entities. Note that a Certification Authority, a Registration Authority or RA- Agents are Entities. The term Entity excludes trusts, partnerships and sole proprietors
FIPS 140-2	Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, 2001

Term	Definition
Hardware Security Module. HSM	A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.
identity authentication	Identity authentication is the process of actually confirming that identity.

Term	Definition
Identity document	An identity document is used to verify aspects of a person's identity. Recognised identity documents for natural persons are; 1. For South African citizens applying from within or outside of the South African Border; 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. 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 c. identity document issued from the authorized government body responsible for issuing identity documents to citizens of the stated country.

Term	Definition
Identity Documents for a company, close corporation or other legal entity	Where the subscriber is a company, close corporation or other legal entity 1. the relevant constitutive documents, 2. resolution or power of attorney of the directors, authorising a specific person to apply for or otherwise deal with LAWtrust in relation to the issuing, renewal or replacement of certificates; and the identity documents applicable for natural persons for each of the directors, members of trustees of the applicant and the authorised key holder together with a resolution appointing the representative as the authorise key holder.
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 for initial registration 2. Accredited certificate for Certificate renewal Where the subscriber is a partnership, 1. the constitutive documents of the partnership, if applicable and 2. the identity documents applicable for natural persons.
Integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
interoperation	In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

Term	Definition
Key Encryption Key or KEK	A key encryption key (KEK) is a cryptographic key that is used for encrypting other cryptographic keys.
key pair	Two mathematically related cryptographic keys, referred to as a private key and a public key, having the properties that (i) one key (the public key) can encrypt a message which only the other key (the private key) can decrypt, and (ii) even knowing the one key (the public key), it is computationally infeasible to discover the other key (the private key).
Key Wrapping	Key wrapping is a cryptographic construct that uses symmetric encryption to encapsulate key material.
LAWtrust AeSign CEN-SSCD RA Charter	the practices and processes that the RA-Agent will follow in performing the certificate lifecycle processes delegated by LAWtrust. Any differences or specific responsibilities will be documented in a variation agreement.
LAWtrust AeSign CEN-SSCD Subscriber Agreement	the terms and conditions governing the use and protection of the certificate by the subscriber and accepted by the subscriber through signing the document
LAWtrust OA	LAWtrust Management forum responsible for the implementation of the LAWtrust Policy and Practices and the Operations of the LAWtrust PKI environment
LAWtrust Operations	the operational certificate support area of LAWtrust
LAWtrust PA	LAWtrust Management forum responsible for defining the LAWtrust Policy and Practices and ensuring that the Policies and Practices are adhered to.

Term	Definition
LAWtrust RA	LAWtrust is a Registration Authority providing Digital Certificate Lifecyle management services to applicants, subscribers and relying parties. LAWtrust may outsource some or all the digital certificate lifecycle responsibilities to separate legal entities. When such an end entity is appointed the entity will be referred to as a LAWtrust RA-Agent
LAWtrust Registration Authority	the LAWtrust management system including policies procedures and technology components used for the management of the AeSign Central SSCD certificate requests, renewals, revocations, etc
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.
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 overall commercial contract between LAWtrust their clients.
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.

Term	Definition
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.
Out-of-band	Out-of-band communication means a mechanism of communication other than the one used for the current transaction. (examples are email, SMS or other mechanism approved by the LAWtrust PA). Any out-of-band communication requires an audit trail in support of evidence that the communication occurred.
PKI	See definition of public key infrastructure.
private key	The key of a key pair used to create a digital signature and is required to be kept secret.
Process Flow Annexure	The description of the process flow and responsibilities between LAWtrust and the RA-Agent stipulating for the management digital certificate lifecycle activities, where such activities vary from a Registration Authority Charter document.
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.
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.

Term	Definition
RA-Agent	the legal entity appointed by LAWtrust to provide authentication of identities and certificate lifecycle functions on behalf of the LAWtrust RA
RACI	A responsibility assignment matrix describes the participation (Responsible, Accountable, Consulted, Inform) by various roles in completing tasks or deliverables for a project or business process. Responsible: The person performing the task Accountable: The person who makes sure that the task is completed. Consulted: Consulted prior to completion of the task (two-way) Inform: Informed of the results (one-way)
RACI Roles for RA Charter and Certificate Lifecycle Management	ADM Administrator APL Applicant AUD Auditor DMA Department Manager ENR Enrolment Officer HL Head of Legal LTW LAWtrust OA Operations Authority PA Policy Authority RAG RA-Agent RA Registration Authority SC Security Committee SD Solutions Director SSO Signing Services Owner SUB Subscriber

Term	Definition
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; LAWtrust may appoint a Third Party as an RA-Agent to perform some or all of the Digital Certificate Lifecyle responsibilities. Such an RA-Agent will be governed by the LAWtrust AeSign CEN-SSCD RA Charter, as a general terms and conditions agreement. Any variations (peculiar to the RA-Agent in question) from the LAWtrust AeSign CEN-SSCD RA Charter, will be documented in a variation agreement as an addendum to this RA Charter.
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
SAAA	South African Accreditation Authority. The office of the South African Accreditation Authority is established in terms of Chapter VI, Part 1 of the Electronic Communications and Transactions Act 25 of 2002. The Authority is responsible for the accreditation of authentication and certification products and services used in support of electronic signatures and monitoring of the activities of authentication and certification service providers whose products or services have been accredited by the South African Accreditation Authority (SAAA) within the Republic of South Africa.

Term	Definition
SCD	Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature
Secure Key Store	Technology component (Software of Hardware) which enables a mechanism to generate, store and use cryptographic keys in a secure manner.
Secure Signature-Creation Device (SSCD)	A secure personalised device with cryptographic capabilities in which a subscriber electronic signature creation data (SCD) will be generated and all encryption operations are performed in the SSCD. SCD generation and use is with sole control of the subscriber.
Secure storage	Secure storage is any storage which preserves the Confidentiality, Integrity and Availability of its contents. Secure storage is required for physical paper documents and electronic documents.
Security Committee	LAWtrust Management Team appointed to oversee Information and Cyber Security activities.
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.
Signing account	The signing account is a is a location on the signing server used to store a user signing credentials and other information. A signing account allows or does not allow a user to connect and use the signing services
SKS	See Secure Key Store
SSCD type 2	SSCD type 2 is in "EN14169-2 Protection Profile Secure signature creation device - Part 2: Device with import of key"

Term	Definition
Subscriber	An Applicant whose digital certificate application has been approved and a digital certificate has been issued to them.
subscriber agreement	An agreement between the certificate authority and a subscriber that sets out the terms and conditions governing the issuance of a certificate, control of the private key that corresponds to the public key listed in the certificate, acceptable use of the certificate, notification of compromise of the private key, and matters ancillary and related thereto.
System	A System is a collection of components (HW, SW, DB, process) organised in a manner to provide specific outcomes.
Trustworthy System	A trustworthy system is 1. A system which is protected against modification and ensures the technical security and reliability of the processes supported by them; 2. Can be used to store data provided to it, in a verifiable form so that: (i) the systems are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity;
Valid digital certificate	A valid digital certificate means that the certificate has not expired, it has not been revoked, or suspended.

Term	Definition
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.

Table 3: Definitions and Acronyms

7. Public Key Infrastructure Configuration

7.1 Applicant and Subscriber

In this Charter, 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 End Entity to whom it has been issued shall be referred to as a "subscriber".

7.2 Eligibility for Certification

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

1. The Applicant has a valid identity document.
2. The Applicant is in good standing with LAWtrust RA or the **Error! Unknown document property name.**.
3. The Applicant is fully aware of the responsibilities regarding the care and use of digital certificates and keys (as contained in the LT_ISP_SIGNINGCA01_CEN-

SSCD_CPS, this Charter, the applicable LAWtrust Subscriber Agreement 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. Digital signing of documents and transactions.

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

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

7.4.1 Trust hierarchy:

1. LAWtrust Root Certification Authority CA2 – Root Certification Authority (RCA)
2. LAWtrust SIGNING CA01 – Local Certification and Issuing Authority (IA)
3. LAWtrust RA – Local Registration Authority (LRA)
4. LAWtrust RA-Agent – Third party appointed by LAWtrust to perform RA duties.

7.5 Certificate Type & Content

7.5.1 Certificate Type

- X.509

7.5.2 Certificate Content End Entity

1. CN=first and surname Applicant.
2. E=email address of Applicant.
3. OU=Organisational unit of Applicant.
4. O=Organisation Name of Applicant as registered.

5. L=Location (Suburb)
6. ST= Location (Province\State)
7. C=Location (Country)
8. SERIALNUMBER=SERIALNUMBER

7.6 Private Key Protection

The LAWtrust SIGNING CA01 will issue LAWtrust SigningCA Certificates to Applicants and the private keys or SCD of these certificates will be protected by the following solution

7.6.1 Subscriber sole control of private key

The SCD will be protected by security controls ensuring that the subscriber maintains sole control of the SCD. Combining the concepts in sections "7.6.1.1 Authentication of Applicant at generation of private key", "7.6.1.2 Authentication scheme for accessing the private key" and "7.6.1.3 Signature service authentication", enhance the security controls to achieve the highest levels of assurance of the user's sole control together with the flexibility of Central Signing.

7.6.1.1 Authentication of Applicant at generation of private key

The Applicant's identity is verified prior to the point where the instruction to generate the private key is initiated by the Applicant and sent to the Signature solution to generate the private key and obtain a certificate from the CA.

The Applicant must be in control of the generation of their private key. This process must include the audit trail of the Applicant's identity being verified, the Applicant being in control of the instruction to generate their private key.

7.6.1.2 Authentication scheme for accessing the private key

The LAWtrust Current authentication mechanisms supported

1. User created PASSWORD: The user creates their own static alpha-numeric PASSWORD associated to the signing key when the key is generated.

2. System generated OTP: A dynamically generated text-based One-Time-Password (OTP)

3. Device authentication : An authentication scheme based on a unique device code linked to the subscriber

4. Other method as approved by the PA and documented in a variation agreement.

Used together the PASSWORD and OTP/Device authentication or other methods are accepted as two factor authentication.

7.6.1.3 Signature service authentication

The access to the signing keys is further enhanced by the authentication of the requester application to the signing application and or API. This is facilitated by using TLS for end entity signing or mutual authentication between the requesting application and the signing application and or API.

7.6.2 Central SSCD

A central SSCD is made available to subscribers provisioned by standards based enhanced HSM key wrapping functionality ensuring that SSCD Type 2 compliant signatures are produced.

7.6.3 Supply of SSCD's

LAWtrust will provide subscribers directly or via **RA-Agent**'s with the following key storage and key generation capabilities

Central SSCD: FIPS 140-2 compliant HSM for key generation and a Type 2 SSCD for key storage

7.7 Secure communication between the RA and the CA

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

- TLS protecting communications between administrator's authentication to the RA.
- Only administrators identified by the RA and authorised by LAWtrust will be provisioned with access to the RA.
- Where the API is used to control digital certificate lifecycle events, the requesting module is authenticated via Mutual Authentication

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

8. Digital Certificate Application Processes

8.1 Digital Certificate Application

8.1.1 Application for a LAWtrust Digital Certificate

The **RA-Agent** shall be entitled to accept and process applications for end entities for the issuance of a LAWtrust Certificate.

The RA or **RA-Agent** shall retain all of the paper based and or electronic documentation relevant to the authentication of the identity of the Applicant as well as the verification of supporting information in secure storage, in conformance with the requirements of the LAWtrust Policy Authority, for a period of at least 7 (seven) years after the expiry or revocation of the LAWtrust Certificate as required by the ECT Act.

8.1.2 End Entity or Natural Person application

As a minimum, the **RA-Agent** shall require from the natural person Applicant:

- A duly completed and signed LAWtrust Subscriber Agreement authorised by the Enrolment Officer.
- A copy of the Applicant's South African Identity Document or Passport.
- An application form which includes the Applicant details to be verified. This may be included in existing paper and or electronic processes.

For purposes of seamless integration with existing processes,

- the application may be combined with the subscriber agreement
- the application may be included in or inferred by a separate onboarding process, such as self enrolment applications.

A secure video session, if deemed necessary, may be established between the RA-agent and the subscriber to perform the identification processes relating to the application of a certificate issued under this charter.

8.2 Digital Certificate Application Verification

During the verification process the Subscriber Agreement and the copy of the identity document and other LAWtrust certificate application documentation should be collected and placed into secure storage.

8.2.1 Process of Certificate Request Verification

The **RA-Agent** appointed Enrolment Officer will perform the following steps to verify the certificate request:

1. Review the Applicant's request for the certificate
2. Receive a LAWtrust Certificate Subscriber Agreement that has been signed by the Applicant.
3. Perform validation of all details to be included in the digital certificate.
4. Perform validation of the subscriber's notification mechanism.
5. Authorize the certificate.
6. Advise the Applicant on the outcome of the Application via the mechanism agreed to in Section 6. Above.

8.2.2 Applicant Identity Verification

The requirements stated below applies to all **RA-Agent**s and any third party performing such tasks on behalf of the LAWtrust RA.

The **RA-Agent** Enrolment Officer will perform the following steps during the identity verification:

1. Perform a face-to-face verification or equivalent (such as a secure video conference) of the Applicant against the provided South African National Identity document/smart ID card or the Passport.
2. Ensure the provided identity document is not counterfeit (the Enrolment Officer must be trained in aspects of detecting false identity documents).
3. Receive a copy of the identity document and confirm it is of the original (if a copy is not made in witness of the Enrolment Officer).
4. Optionally capture a photograph of the Applicant's face.

8.3 Digital Certificate Certification

8.3.1 Process of Secure Key Store Issuance and Registration

Once the verification is successful, the **RA-Agent** appointed administrator will perform the following steps to personalize and register a Secure Key Store to an Applicant:

1. Create a Signing account
2. Populate the account with the Applicant's details
3. Issue the instruction to send the complete registration link to the Applicant.

Where the API is used to control digital certificate lifecycle events, the request to create a signing account are sent to LAWtrust via the API itself.

8.3.2 LAWtrust Certificate Issuance Process

The **RA-Agent** will perform the following steps to issue a certificate:

1. Enrol the Applicant on the LAWtrust Signing Application using the Applicant's information as it appears on the application.

2. The required keys will be generated in the HSM and the LAWtrust certificate will be stored on the subscriber's central SSCD. At this point the Applicant is now a subscriber.

3. **RA-Agent** shall, if required by the subscriber, provide telephonic assistance to the subscriber for the use of the LAWtrust Certificate.

Where the API is used to control digital certificate lifecycle events, the request to create a signing account is facilitated via the LAWTrust API.

8.3.3 Digital Certificate Acceptance

After the issuance of the LAWtrust Certificate to the subscriber, 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.

8.3.4 Advising on the Outcome of the Application

When the application is granted, in the case of the LAWtrust Signing Portal the Applicant receives a link to complete the registration or in the case of the API, a notification that the signing account is ready for use is sent to the subscriber.

The receipt of the link or the notification of ready to use, serves as notification that the application was granted. If the application is not granted then the "complete registration" link or the ready to use notice will not be sent and the **RA-Agent** Enrolment Officer will inform the Applicant.

The **RA-Agent** will give notice to the Applicant of the refusal to issue a LAWtrust Certificate during the enrolment process if the requirements are not met.

8.4 Digital Certificate Reliance

8.4.1 Certificate use verification

The certificate validity can be verified via the CRL or via OCSP ath the URLs specified in the certificates themselves and/or CPS. OCSP is available for the certificate validity information to be included in the electronic signature.

8.5 Time to process certificate applications

8.5.1 Certificate Authority

The **LAWtrust SIGNING CA01** will process a CSR immediately on receiving such a request.

8.5.2 Registration Authority

The LAWtrust RA will process an application in line within 24 hours of receipt of the request from the **RA-Agent**.

8.6 Proving possession of private key

For Central SSCD the private signing key is generated by LAWtrust, on behalf of the subscriber. The Subscriber is the only person who has access to the authentication credentials.

9. Digital Certificate status changes

9.1 Rename user (change user CN)

When a Subscriber user's common name changes, e.g. a fa subscriber gets married and their 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.

9.1.1 Process for certificate contents changes

1. Subscriber submits an application to the Enrolment Officer. (New certificate application)
2. Enrolment Officer follows the process of a new application.
3. The old certificate will be revoked prior to the new certificate being issued.

In the case of the API, the process is facilitated via the LAWTrust API.

9.2 LAWtrust Certificate Revocation and Suspension

9.2.1 Circumstances for revocation and suspension

Any LAWtrust Certificate may be revoked or suspended if any of the following circumstances have occurred or suspected:

LAWtrust Certificates may be revoked with authority from the LAWtrust Operations Authority under the following circumstances:

1. Abuse of the digital certificate by the subscriber.
2. Subscriber's request.
3. Any change in the information contained in the LAWtrust Certificate issued to a Subscriber;
4. Subscriber suspected of fraudulent activity.
5. The compromise of the **LAWtrust SIGNING CA01** private key, or if applicable, the compromise of a superior Certification Authority's private key;

6. Breach by the Subscriber of any of the terms of this LAWtrust SIGNING CA01 CEN-SSCD RA Charter or the Subscriber Agreement entered into with the Subscriber;
7. Non-payment of fees in respect of any services provided by LAWtrust or **RA-Agent**.
8. Issue or use of the certificate not in accordance with the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS.
9. If a subscriber dies and after receiving a certified copy of the subscriber's death certificate.
10. On receipt of documentary proof that a subscriber that is a legal person has been wound up, or deregistered or has ceased to exit.
11. The LAWtrust SIGNING CA01 or LAWtrust Root CA2 (4096) expires.
12. A determination by the LAWtrust SIGNING CA01 or a **RA-Agent** that the certificate was not issued in accordance with this LT_ISP_SIGNINGCA01_CEN-SSCD_CPS or the provisions of the Subscriber's Agreement entered into with the Subscriber;
13. Any change in the operation of the RA, RA-agent, subscriber affiliation, or in the case of the Signing service, changes to the subscriber account information, that may result in a revocation or suspension of the subscriber certificate.
14. Any other reason that the LAWtrust SIGNING CA01 reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust Certificate.

9.2.2 LAWtrust Certificate Revocation Process

A request to revoke a LAWtrust Certificate may be submitted by a Subscriber to the **RA-Agent** or by the **RA-Agent** to the LAWtrust RA or by the LAWtrust SIGNING CA01 if any of the circumstances in clause 9.2.1 occurs.

The appointed Enrolment Officer will perform the following steps to revoke the Subscriber's LAWtrust Certificate:

1. The Enrolment Officer will log on to the LAWtrust SIGNING CA01 Administration Portal Perform the following identity verification for the Subscriber if the revocation request was submitted by the Subscriber:

    a. Retrieve the identity information of the Subscriber from the LAWtrust database; and

    b. Verify that the subscriber exists and that the reasons for revocation are valid by verifying with the **RA-Agent**.

2. Delete the signing account which issues a revocation request with the relevant revocation reason.

3. The LAWtrust SIGNING CA01 shall within 24 hours of receiving a revocation request, post the serial number of the revoked LAWtrust Certificate to the CRL and publish it as documented in clause 8.4.

4. The **RA-Agent** shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust Certificate has been revoked. This notification could be via email of via a means which an event can be logged in an audit trail.

Where the API is used to control digital certificate lifecycle events, the request to revoke a digital certificate (steps 1 and 2) are facilitated via the LAWTrust API.

Revocation of a LAWtrust Certificate shall not affect any of the Subscriber's contractual obligations under the LAWtrust Subscriber Agreement entered into by the Subscriber.

9.3 LAWtrust Certificate Suspension

The LAWtrust Signing Portal does not offer certificate suspension. It offers account suspension which does not suspend the Certificate. Conversely the Integration via the API does allow for Certificate suspension.

Where the API is used to control digital certificate lifecycle events, the request to suspend a digital certificate is facilitated via the LAWTrust API.

9.4 LAWtrust Certificate Re-Instatement

9.4.1.1 Circumstances for lifting certificate suspension

The LAWtrust Signing Portal does not offer certificate reinstatement. It offers account reinstatement which does not affect the Certificate. Conversely the Integration via the API does allow for Certificate re-instatement or lifting of suspension.

9.4.2 LAWtrust Certificate Re-Instatement process

A request to lift the suspension on a LAWtrust Signing Account may be submitted by the LAWtrust RA, an Agent appointed by LAWtrust or the LAWtrust SIGNING CA01 if reason is provided that the certificate must be re-instated for the intended use by the Subscriber.

The RA Enrolment Officer will perform the following steps to lift the suspension of the Subscriber signing account:

1. The LAWtrust appointed Enrolment Officer will log on to the LAWtrust SIGNING CA01 Administration Portal and issue an un-hold (lift suspension) request for the specific signing account.
2. The LAWtrust SIGNING CA01 shall within 24 hours of receiving an un-hold request, reinstate the signing account.
3. The LAWtrust appointed **RA-Agent** shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust signing account has been reinstated (un-suspended).

Where the API is used to control digital certificate lifecycle events, the request to re-instate the digital certificate (steps 1 and 2) are facilitated via the LAWTrust API.

9.5 LAWtrust Certificate Renewal

The CA and the RA shall maintain controls to provide reasonable assurance that certificate renewal requests are accurate, authorized and complete.

9.5.1 Automatic Renewal

The LAWtrust Certificate can be renewed on the approach of the expiry date for the certificate. The autorenewal is allowed when the subscriber agrees to the certificate being automatically renewed prior to the certificate expiry.

Once the digital certificate has been renewed, the **RA-Agent** shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust Certificate has been renewed. This notification should be via a means which can be demonstrated and an event can be logged in an audit trail.

The controls for manual renewal are included in the list below;

9.5.1.1 Certificate auto-renewal process

The LAWtrust Certificate will be renewed on the approach of the expiry date for the certificate. The renewal of certificates will be managed by the LAWtrust RA or the **RA-Agent**

During a certificate renewal the certificate may be renewed using the same key pair or may be renewed with a re-key and the new public key information will be included in the new LAWtrust Certificate.

9.5.2 Manual Renewal

The controls for manual renewal are included in the list below;

9.5.2.1 Certificate manual renewal process

1. The certificate renewal Process should include an attestation whether the subscriber is currently authorized for the digital signing operations.

Where the API is used to control digital certificate lifecycle events, the request to renew the digital certificate is facilitated via the LAWTrust API.

9.6 LAWtrust Certificate re-key

Certificate re-key occurs when a certificate is requested post expiry, post revocation or during a name change. In the case where there is a certificate re-key required, the following full registration process will be followed, as per section 8.

Where the API is used to control digital certificate lifecycle events, the request to re-key the digital certificate is facilitated via the LAWTrust API.

9.6.1 Re-Key After Expiry

If an Applicant has previously been issued with a Signing account and associated digital certificate and the digital certificate has been revoked, then the Applicant will need to follow the process as if they were a first-time Applicant. (full identity verification etc), see section 8.

9.6.2 Re-Key After Revocation

If an Applicant has previously been issued with a Signing account and associated digital certificate and the signing account has been deleted which results in a digital certificate revocation, then the Applicant will need to follow the process as if they were a first-time Applicant. (full identity verification etc), see section 8.

9.6.3 Re-Key After Name Change

If a subscriber requests certificate contents changes for example a Name change, a rekey is required and the Applicant will need to follow the process as if they were a first-time Applicant. (full identity verification etc), see section 8.

10. SCCD Lifecycle Management

10.1 Subscriber private key generation and storage

The subscriber's private key must be generated under the sole control of the subscriber.

The private key can be stored in the following approved key stores

1. On a central SSCD

10.2 Life cycle management of the SSCD.

10.2.1 Central SSCD

Central SSCDs are created in the following manner

1. The central SSCD's consist of a database entry including the following items
    a. Subscriber private key encrypted with a KEK

b. Public key certificate

2. Central SSCDs are created when the subscriber is enrolled.

3. If the SSCD is suspected to be compromised, the certificate is revoked and a new SSCD created following the process in section 8.

4. If a subscriber has a change in job status, which does not require the use of the certificate and a validated revocation request is received by an approved **RA-Agent**, the signing account is deleted and the certificate is revoked.

10.3 LAWtrust SSCD PASSWORD Reset

If a LAWtrust Certificate Subscriber forgets their PASSWORD to access the private signing key, then the following process will be followed to reset the PASSWORD:

1. The subscriber will use the self-service portal to reset the PASSWORD.

Where the API is used to control digital certificate lifecycle events, the request to reset the signing account password is facilitated via the LAWtrust API.

10.4 LAWtrust Mobile Number Reset

If a LAWtrust Certificate Subscriber requests a mobile number used for OTP to change then the following process will be followed to reset the mobile number:

1. In the case of the LAWtrust Signing Portal, the subscriber will use the self-service portal to reset the mobile number.

Where the API is used to control digital certificate lifecycle events, the request to reset the subscriber mobile number is facilitated via the LAWtrust API.

11. Other responsibilities of the Error! Unknown document property name.

11.1 Audit trails

All supporting documentation which can be used as evidence that the **RA-Agent** responsibilities occurred must be held in secure storage and be made available for any audit request by the LAWtrust RA.

11.2 Confidentiality

LAWtrust and all **RA-Agent**s shall use commercially reasonable care to prevent such information used and stored for the purpose of issuing digital certificates, from being used or inappropriately disclosed for purposes other than those described in this Charter, the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS, Subscriber's Agreement or Relying Party Agreement.

11.3 Annual Audit

See section 13.

11.4 Other

No stipulation.

12. Termination of RA Responsibilities

During the course of day to day business, if there is a requirement to terminate an **RA-Agent** as a third party performing some or all of LAWtrust RA responsibilities, the following process will be followed.

12.1 Circumstances for termination

LAWtrust may terminate the appointment of the **Error! Unknown document property name.** under any of the following conditions

1. When the contract between the two entities lapses or is terminated at the request of either party.

2. When there is a material breach or failure of the **RA-Agent** to adhere to the responsibilities and obligations of the RA charter.

3. When LAWtrust, after conducting RA audits, deems it necessary to terminate or withdraw such an appointment

4. Any other event that LAWtrust deems necessary to warrant such a termination, which may include but is not limited to:

    a. Failure to provide access to information required for audit purposes

    b. Failure to exercise required controls over digital certificate usage

    c. Failure to make payment

    d. Regulatory requirements

    e. Using of certificates for fraudulent purposes

12.2 Communication

1. Inform all stakeholders of the intent to terminate the **RA-Agent** services.
2. Stakeholders will include the RA Agent, any third party appointed by the RA-Agent to manage the process, the LAWtrust PA and the LAWtrust OA.

12.3 Planning

1. The LAWtrust RA and the **RA-Agent** must agree on the sequence of events resulting in the termination.
2. The LAWtrust RA and the **RA-Agent** must agree on the most appropriate timing for the termination of the services.

12.4 Data Management

1. Ensure that the **RA-Agent** and or LAWtrust has access to all information relating to the identity verification and digital certificate lifecycle management process for a period of 7 (seven) years.

2. Ensure that the information is deleted after the agreed period of 7 (seven) years.

13. RA-Agent Annual Audit

LAWtrust may perform a pre-audit in preparation for a formal audit by an auditor authorised by the SAAA. The frequency of these formal audits is expected to be once per calendar year for compliance with the practices and procedures set out in this Charter and the LT_ISP_SIGNINGCA01_CEN-SSCD_CPS.

LAWtrust shall provide a notice period of 30 days of its intent to perform such an audit. LAWtrust may include a third party to perform such audits.

The RA-Agent must cooperate with such pre-audit and formal audit proceedings and make available such information as is reasonably required by auditors. The **RA-Agent** shall provide LAWtrust and or an appointed auditor with reasonable access to the evidence supporting that the **RA-Agent** responsibilities were performed. This includes all documentation used in the verification process and stored by the RA Agent.

If the results of an audit report recommend remedial action, the LAWtrust RA and or the **RA-Agent** shall implement corrective action within 30 (thirty) days of receipt of such audit report. Failure to remediate in that period may lead to the suspension of the services by LAWtrust.

14. References

Reference	Details
CA Policies, Practices & Agreements:	LAWtrust SIGNING CA01 Certificate Practices Statement (https://www.lawtrust.co.za/repository). LAWtrust Digital Signature Subscriber Agreement (https://www.lawtrust.co.za/repository). LAWtrust Relying Party Agreement (https://www.lawtrust.co.za/repository).
Legal Framework	Electronic Communications and Transactions Act of 2002 and relevant Regulations
RA and RA-Agent Responsibilities	RA versus RA-Agent Responsibilities Matrix

15. SIGN OFF ACCEPTANCE

Name:	Katekani Hlabathi
Authority:	Policy Authority
Title:	Chief Information Officer
Date:	2020-11-02
Signature: