https://www.lawtrust.co.za	**Classification**	**LEVEL 1: PUBLIC INFORMATION**
	Reference	**LT_AUTH CA02_RAC_V005 2026-09-30**
	Location	**https://www.lawtrust.co.za/repository**
	Version	**V005 2026-09-30**
	Policy Authority	**LAWtrust PA**

LAWtrust AUTH CA02 Registration Authority Charter (LAWtrust AUTH CA02 RA Charter)

Law Trusted Third Party Services (Pty) Ltd

Registration number 2001/004386/07

("LAWtrust")

20 Woodlands Drive,

Woodlands Office Park, Woodmead,

Johannesburg, 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

COPYRIGHT NOTICE

LAW TRUSTED THIRD PARTY (PTY) LTD ("LAWTRUST") RETAINS THE COPYRIGHT IN THIS REGISTRATION AUTHORITY CHARTER ("RAC") AS WELL AS ANY NEW VERSIONS OF IT PUBLISHED AT ANY TIME BY LAWTRUST.

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

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

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V001 2020-11-02	2020-11-02	K Hlabathi	New version	Expired
V002 2023-09-30	2023-10-31	M De Waal	Yearly review, address change, format changes	Expired
V003 2024-09-30	2024-10-31	M De Waal	Yearly review	Expired
V004 2025-09-30	2025-10-31	M De Waal	Yearly review	Expired
V005 2026-09-30	2026-10-31	M De Waal	Yearly review	Current

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 AUTH CA02 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 8

2. SCOPE 8

3. Registration Authority Appointment 9

4. Document name and publication 10

5. Charter Responsibilities 11

6. Definitions and Acronyms 13

7. Public Key Infrastructure Configuration 27

7.1 Applicant and Subscriber 27

7.2 Eligibility for Certification 27

7.3 Purpose of Certification 27

7.4 PKI Hierarchy – CA's, RA and private keys 28

7.4.1 Trust hierarchy: 28

7.5 Certificate Type & Content 28

7.5.1 Certificate Type 28

7.5.2 Certificate Content (Subject details) 28

7.6 Private Key Protection 28

7.7 Secure communication between the RA and the CA 29

8. Digital Certificate Application Processes 29

8.1 Digital Certificate Application 29

8.1.1 Application for a LAWtrust Digital Certificate 29

8.1.2 End Entity or Natural Person application 29

8.2 Digital Certificate Application Verification 30

8.3 Process of Enrolment (account creation) 31

8.3.1 Required fields 31
8.3.2 Prerequisites 31
8.3.3 Account creation 31
8.4 Certificate Issuance Process 31
8.4.1 Enterprise Certificate with ESP 31
8.4.2 Enterprise Certificate on Web Portal 32
8.4.3 API Integration 33
8.5 Digital Certificate Acceptance 33
8.6 Advising on the Outcome of the Application 33
8.7 Digital Certificate Reliance 34
8.7.1 Certificate use verification 34
8.8 Time to process certificate applications 34
8.8.1 Certificate Authority 34
8.8.2 Registration Authority 34
9. Digital Certificate status changes 34
9.1 Rename user (change user CN) 34
9.1.1 Process for certificate contents changes 34
9.2 Circumstances for Revocation and Suspension Certificates 35
9.2.1 Certificate Revocation Processes 36
9.2.2 Conditions for Certificate Suspension 36
9.2.3 Certificate Suspension Processes 37
9.3 LAWtrust Certificate Re-Instatement 37
9.4 LAWtrust Certificate Renewal process 38
9.5 LAWtrust Enterprise Certificate Recovery 38
10. Other responsibilities of the RA-Agent 39
10.1 Audit trails 39

10.2 Confidentiality 39

10.3 Annual Audit 40

10.4 Other 40

11. Termination of RA Responsibilities 40

11.1 Circumstances for termination 40

11.2 Communication 41

11.3 Planning 41

11.4 Data Management 41

12. RA-Agent Annual Audit 41

13. References 42

14. SIGN OFF ACCEPTANCE 43

1. INTRODUCTION

Law Trusted Third Party Services (Pty) Ltd ("LAWtrust"), a wholly owned subsidiary of Altron TMT (Pty) Ltd, is the owner and custodian of information that is critical to its PKI business.

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 (LAWTrust AUTH CA02 CPS). Combined, this Charter and the LAWTrust AUTH CA02 CPS specify the digital certification process for the issuance and management of LAWtrust Digital certificates. All persons are required to adhere to the terms and conditions contained in the LAWTrust AUTH CA02 CPS as well as any other requirements imposed by LAWtrust that do not conflict with the LAWTrust AUTH CA02 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 to facilitate the LAWtrust digital lifecycle responsibilities via an API or through a manual issuance process.

3. Registration Authority Appointment

Law Trusted Third Party Services (Pty) Ltd ("LAWtrust"), a wholly owned subsidiary of Altron TMT (Pty) Ltd, is the owner and custodian of information that is critical to its PKI business.

LAWtrust operates a Registration Authority (LAWtrust Auth CA02 RA) to perform identity verification and manage the digital certificate lifecycle. The terms and conditions for operating a Registration Authority issuing LAWtrust Authentication Certificates are documented in this LAWtrust AUTH CA02 RA Charter. The LAWtrust Auth CA02 RA, operated by LAWtrust, is responsible for managing digital certificate lifecycles and is bound by the terms and conditions in this LAWtrust AUTH CA02 RA Charter.

LAWtrust may appoint a third party referred to as an RA-Agent to perform some or all the responsibilities of the LAWtrust Auth CA02 RA. This LAWtrust AUTH CA02 RA Charter serves as the documented responsibilities of the LAWtrust Auth CA02 RA and any appointed RA-Agent. Where deviations from this LAWtrust AUTH CA02 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 RA-Agent includes the following:

1. LAWtrust will verify the identity of the legal entity performing the RA-Agent responsibilities using clause 3.2.2 of the LAWTrust AUTH CA02 CPS.

2. LAWtrust and the **RA-Agent** will agree on the RA-Agent authentication mechanisms when requesting certificate and signature services.

At a high level, the **RA-Agent** will:

RA Capability [RA-Agent Responsibilities]		**RACI**			
		R	**A**	**C**	**I**
1.	Accept applications for LAWtrust AUTH CA02 Certificates.	AG	LT	SU	SU
2.	Perform authentication of identities and verification of information submitted by Applicants when applying for the issuance of a digital certificate by the LAWtrust AUTH CA02 in terms of the provisions of this LAWtrust AUTH CA02 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 AUTH CA02, in accordance with the provisions of this LAWtrust AUTH CA02 RA Charter and the LAWTrust AUTH CA02 CPS.	AG	LT	SU	SU

Table 1: RA Agent Responsibilities (high-level)

4. Document name and publication

This document is the LAWtrust AUTH CA02 Registration Authority Charter (LAWtrust AUTH CA02 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 LAWTrust AUTH CA02 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 Auth CA02 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.
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.
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 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.
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.
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
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.
Administrator	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
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.
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.
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.
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.
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.
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.
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 ADM Administrator 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
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.

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"
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.
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 has a valid email account.
3. The Applicant is in good standing with LAWtrust Auth CA02 RA or the RA-Agent.
4. The Applicant is fully aware of the responsibilities regarding the care and use of digital certificates and keys (as contained in the LAWTrust AUTH CA02 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. Authentication to business systems
2. File and Folder encryption

The above will ensure authentication, authorization, privacy 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 2048 – Root Certification Authority (RCA)
2. LAWtrust AUTH CA02 – Local Certification and Issuing Authority (IA)
3. LAWtrust Auth CA02 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 v3 certificates that support either a single pair or dual pair

7.5.2 Certificate Content (Subject details)

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 Authentication Certificates are protected with the Entrust Entelligence Security Provider as the secure key store or the operating system Key Store. Access to the private key is via a password which the subscriber has knowledge of.

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 LAWtrust Auth CA02 RA shall be entitled to accept and process applications for Entities and End Entities for the issuance of a LAWtrust Certificate.

8.1.2 End Entity or Natural Person application

The LAWtrust Auth CA02 RA verify the Applicant's identity using the possession of a reliable form of identification. Personal identifying information shall be compared with Applicant-provided information to confirm that the asserted name matches:

(a) The name contained in the presented identification credential

(b) The unique identifier to be used in the CN of the certificate

(c) A current address, or phone number or email sufficient to identify a unique individual or entity.

8.2 Digital Certificate Application Verification

The LAWtrust Auth CA02 RA shall verify the applicant's information by any of the following means:

1 In-person proofing before an RA or Trusted Agent with presentment of a valid current government-issued identity document that contains the Applicant's picture and either address of record or nationality (e.g. driver's license or ID Document). Such authentication does not relieve the RA of its responsibility to verify the presented data.

2 Remotely verifying information provided by the Applicant. The Issuer CA or RA may confirm an address by issuing the credentials in a manner that confirms the address of record or verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records that are available to the Issuer CA or RA.

3 The Issuer CA or RA may confirm an address by issuing the credentials in a manner that confirms the address of record or verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number or email by sending a challenge-response SMS message or email with the applicant in records that are available to the Issuer CA or RA.

4 If the Issuer CA or RA has a current, ongoing relationship with the Applicant, the Issuer CA or RA may verify identity using an exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo ID, and (b) the ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.

8.3 Process of Enrolment (account creation)

8.3.1 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)

8.3.2 Prerequisites

Once the verification was successful the application can be submitted to the CA.

8.3.3 Account creation

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

1. Log on to the LAWtrust AUTH CA02 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 LAWtrust AUTH CA02 AdminServices Portal.
3. Share Authorisation and Reference codes with the relevant party.

8.4 Certificate Issuance Process

8.4.1 Enterprise Certificate with ESP

The LAWtrust Auth CA02 RA appointed administrator will perform the following steps with the Applicant to issue the LAWtrust Auth CA02 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 LAWtrust Auth CA02 RA Certificate was successfully installed on ESP
5. Allow the Subscriber to view the LAWtrust Auth CA02 RA Certificate detail via ESP.
6. If the details on the certificate are incorrectly captured, the LAWtrust administrator 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 LAWtrust AUTH CA02 Certificate.

8.4.2 Enterprise Certificate on Web Portal

The LAWtrust Auth CA02 RA appointed administrator will perform the following steps with the Applicant to issue the LAWtrust Auth CA02 RA Certificate:

1. Change the settings on the web browser if needed
2. Access the Certificate Enrollment Portal
3. Enter the Reference Number and Authorisation Code captured during the Applicant account creation process for the Applicant.
4. Ensure the LAWtrust Auth CA02 RA Certificate was successfully downloaded to the desktop
5. Install the downloaded certificate into the operating system keystore
6. Allow the Subscriber to view the LAWtrust Auth CA02 RA Certificate detail via the browser
7. If the details on the certificate are incorrectly captured, the LAWtrust administrator shall revoke the certificate immediately following the Revocation Process and restart the process of issuance.
8. Assist the Subscriber to test the use of the LAWtrust AUTH CA02 Certificate.

8.4.3 API Integration

During API Integration the integrated system will interact with the CA to issue the certificate and the following steps will be followed.

1. User will be added to the integrated system and the process will be started to create the user on the system.
2. The system will create the CSR on the user's environment and send that through to the system to the connected CA via the secure channel
3. The CA will create the user, and sign the CSR
4. The certificate will then be sent back to the user via the secure channel
5. The integrated system will then install the certificate on the user workstation for future use.

8.5 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.

8.6 Advising on the Outcome of the Application

When the application is granted or declined, the RA-Agent shall notify the subscriber via email or any other commercially feasible means of the outcome of the application process.

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.

8.7 Digital Certificate Reliance

8.7.1 Certificate use verification

The certificate validity can be verified via the CRL or via OCSP at 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.

8.8 Time to process certificate applications

8.8.1 Certificate Authority

The LAWtrust AUTH CA02 will process a CSR immediately on receiving such a request.

8.8.2 Registration Authority

The LAWtrust Auth CA02 RA will process an application in line within 24 hours of receipt of the request from the RA-Agent.

9. Digital Certificate status changes

9.1 Rename user (change user CN)

When a Subscriber user's common name changes, e.g. e female subscriber gets married and their surname changes, the administrator 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 administrator. (New certificate application)

2. Administrator follows the process of a new application.

3. The old certificate will be revoked prior to the new certificate being issued.

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 LAWtrust AUTH CA02 Certificate issued to a Subscriber;
4. Subscriber suspected of fraudulent activity.
5. The compromise of the LAWtrust AUTH CA02 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 Auth CA02 RA 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 LAWtrust AUTH CA02 or LAWtrust Root Certification Authority 2048 expires.
12. A determination by the LAWtrust AUTH CA02 or a LAWtrust Auth CA02 RA that the certificate was not issued in accordance with this LAWtrust AUTH CA02 RA Charter or the provisions of the Subscriber's Agreement entered into with the Subscriber; or
13. Any other reason that the LAWtrust Auth CA02 RA reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust AUTH CA02 Certificate.

9.2.1 Certificate Revocation Processes

A request to revoke a LAWtrust Certificate may be submitted by a subscriber, the LAWtrust Auth CA02 RA or the LAWtrust AUTH CA02 if any of the above occurs.

1 The LAWtrust Auth CA02 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 LAWtrust Auth CA02 RA will send a revocation request to the LAWtrust AUTH CA02.

3 The LAWtrust AUTH CA02 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 LAWtrust Auth CA02 RA shall make a commercially reasonable effort to notify the subscriber via email or any other commercially feasible means.

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.

9.2.2 Conditions for Certificate Suspension

The LAWtrust Auth CA02 RA may suspend a LAWtrust Certificate if:

1 The subscriber is not in good standing with the LAWtrust Auth CA02 RA or LAWtrust AUTH CA02;

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 LAWtrust Auth CA02 RA may request the LAWtrust AUTH CA02 to suspend a LAWtrust Certificate without prior notice to the subscriber.

9.2.3 Certificate Suspension Processes

A request to suspend a LAWtrust Certificate may be submitted by a subscriber the LAWtrust Auth CA02 RA or the LAWtrust AUTH CA02 if any of the conditions listed in section 9.2.2 Conditions for Certificate Suspension are met.

1 The LAWtrust Auth CA02 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 LAWtrust Auth CA02 RA will send a suspension request to the LAWtrust AUTH CA02.

3 The LAWtrust AUTH CA02 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 LAWtrust Auth CA02 RA shall notify the subscriber via email or any other commercially feasible means, 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.

9.3 LAWtrust Certificate Re-Instatement

A request to un-suspend a LAWtrust Certificate may be submitted by a subscriber, the LAWtrust Auth CA02 RA or the LAWtrust AUTH CA02 if all parties are in agreement that the reason for the initial suspension of the certificate has been resolved.

The LAWtrust Auth CA02 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 LAWtrust Auth CA02 RA will send an un-suspend request to the LAWtrust AUTH CA02.

The LAWtrust AUTH CA02 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 LAWtrust Auth CA02 RA shall notify the subscriber via email or any other commercially feasible means that the LAWtrust Certificate has been un-suspended.

9.4 LAWtrust Certificate Renewal process

Prior to the certificate expiring, the RA will notify subscribers via email or any other commercially feasible means, 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 LAWtrust Auth CA02 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.

The LAWtrust Auth CA02 RA shall notify the subscriber via email or any other commercially feasible means that the LAWtrust Certificate has been renewed.

9.5 LAWtrust Enterprise Certificate Recovery

The LAWtrust enterprise (ESP) certificates can be used to encrypt data. When a user loses their epf or pfx 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 LAWtrust Auth CA02 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 LAWtrust Auth CA02 RA will send a recover (reset) request to the LAWtrust AUTH CA02.

4 The LAWtrust Auth CA02 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 LAWtrust Auth CA02 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.

10. Other responsibilities of the RA-Agent

10.1 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.

10.2 Confidentiality

LAWtrust and all RA-Agents 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 LAWTrust AUTH CA02 CPS, Subscriber's Agreement or Relying Party Agreement.

10.3 Annual Audit

See section 12.

10.4 Other

No stipulation.

11. 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.

11.1 Circumstances for termination

LAWtrust may terminate the appointment of the RA-Agent 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

11.2 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.

11.3 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.

11.4 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.

12. 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 LAWTrust AUTH CA02 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 Auth CA02 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.

13. References

Reference	Details
CA Policies, Practices & Agreements:	LAWtrust AUTH CA02 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

14. SIGN OFF ACCEPTANCE

Name:	Marcile De Waal	Jacques Van Zyl
Authority:	Policy Authority	Operational Authority
Title:	Senior Specialist: Policy Authority and Assurance	Head: Technology Operations
Date:	22/10/26	23/10/26
Signature:		Signed by:Jacques Van Zyl Signed at:2026-10-23 07:26:31 +02:00 Reason:I approve this document 