https://www.lawtrust.co.za	Classification	LEVEL 1: PUBLIC INFORMATION
	Reference	LT_PRO_IS_CHA_AeSign_CA V005 2017-10-30
	Location	https://www.lawtrust.co.za/repository
	Version	V005 2017-10-30
	Policy Authority	LAWtrust PA

LAWtrust AeSign CA Registration Authority Charter (LAWtrust AeSign RA Charter)

This Version is Applicable from Effective Date

LAWtrust

Building C, Cambridge Park,
5 Bauhinia Street,
Highveld Park, South Africa, 0046

Phone +27 (0)12 – 676 9240 • Fax +27 (0)12 – 665 3997
Website: https://www.lawtrust.co.za/

DOCUMENT CONTROL

Document history

Version Number	Effective Date	Author	Summary of Changes	Status
V1.0 05-04-2012	05/04/2012	Niel van Greunen	Updated to a new format and logos. General update of certificate lifecycle function. Included audit requirement.	V1.0 05-04-2012
V2.0 05-12-2014	05/12/2014	Niel van Greunen	Review, logo changes and some process updates.	V2.0 05-12-2014
V3.0 30-11-2015	01/12/2015	Bruce Anderson	Review and some process updates.	V3.0 30-11-2015
V004 2017-02-27	2017-02-27	Bruce Anderson	Review and some process updates. Additional review based on AeSign CPS S01	Expired
V005 2017-10-26	2017-10-26	Bruce Anderson	2017 Review	Published

Table of Contents

1. Introduction

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

LAWtrust, in 2012, became the first company in South Africa to be accredited by the Department of Communications 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 AeSign Certification Practice Statement (LAWtrust AeSign CPS). Combined, this Charter and the LAWtrust AeSign CPS specify the digital certification process for the issuance and management of advanced electronic signature certificates and provide the required trust in LAWtrust as an advanced electronic signature digital certificate issuer. All persons are required to adhere to the terms and conditions contained in the LAWtrust AeSign CPS as well as any other requirements imposed by LAWtrust that do not conflict with the LAWtrust AeSign CPS.

2. Scope

This document is part of the LAWtrust Information Security Policy and is applicable to LAWtrust as well as to all parties taking part in the LAWtrust Advanced Electronic Signatures digital certification process.

3. Registration Authority Appointment

LAWtrust is appointed the Advanced Electronic Signature Registration Authority (LAWtrust AeSign RA) to:

1. Accept applications for LAWtrust AeSign Certificates.

2. Perform authentication of identities (face-to-face) 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 AeSign CA in terms of the provisions of this Charter, which has been approved by the LAWtrust Policy Authority.

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

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

4. Document name and publication

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

5. Ownership of Charter

The LAWtrust Operations Authority (OA) is responsible for the upkeep of this Charter. Changes to this Charter are to be authorised by the LAWtrust Operations Authority and approved by the LAWtrust Policy Authority.

The LAWtrust Operations Authority takes full responsibility for the upkeep and content of this Charter, but limits its liability to the use of this Charter as described in the LAWtrust AeSign CPS, this Charter and any other LAWtrust governance policies.

The day to day business operations related to certificate lifecycle would be executed by LAWtrust Operations.

The technical operations related to certificate lifecycle would be executed by the LAWtrust Operations.

6. Definitions and Acronyms

This LAWtrust AeSign RA Charter 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.

Item	Definition
AeSign Certificate	see Advanced Electronic Signature Certificate
Advanced Electronic Signature Certificate	a certificate issued by the LAWtrust AeSign CA and stored in accordance with the prescriptions in the ECT Act and used by a subscriber to generate advanced electronic signatures
AeSign Enrolment Portal	a custom certificate enrolment portal where a subscriber will be able to download a new AeSign certificate onto their Secure Key Store
Client SSCD	Client SSCD is one which is issued to a subscriber and the SSCD is maintained by the subscriber. The client SSCD will have the subscriber electronic signature data (SCD) generated on the SSCD and all encryption operations are performed on the SSCD. SCD generation and use is within sole control of the subscriber.
CSR	see Certificate Signing Request

Item	Definition
Certificate Signing Request	a certificate signing request generated by either the legal entity applicant's browser or the Connect: Direct server to be used by the legal entity applicant that will result in the LAWtrust AeSign RA Charter issuing a certificate to the legal entity applicant
electronic signature creation data or SCD	"electronic signature creation data" means unique data which is used by the signatory to create an electronic signature
End Entity	certificate subject that uses its private key for purposes other than signing certificates, e.g a natural person
Entity	An individual or natural person or an entity that is registered with CIPC are examples of entities. Note that a Certification Authority, a Registration Authority or an End Entity are Entities. The term Entity excludes trusts, partnerships and sole proprietors
FIPS 140-2	Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, 2001
LAWtrust AeSign 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 AeSign RA	see LAWtrust Advanced Electronic Signatures Registration Authority
LAWtrust Advanced Electronic Signatures Registration Authority	the legal entity appointed by LAWtrust to provide certificate lifecycle functions on behalf of the LAWtrust AeSign CA

Item	Definition
LAWtrust Advanced Electronic Signatures Registration Authority Charter	the practices and processes that the LAWtrust RA will follow in performing the certificate lifecycle processes delegated by LAWtrust to the LAWtrust AES RA
LAWtrust AeSign CPS	see LAWtrust Advanced Electronic Signature Certification Practice Statement
LAWtrust Advanced Electronic Signature Certification Practice Statement	the practices that the LAWtrust AeSign Certificate Authority have to employ for certificate lifecycle management, and further includes the terms and conditions under which the LAWtrust AeSign RA Charter make such services available
LAWtrust CMS	see LAWtrust Certificate Management System
LAWtrust Certificate Management System	the LAWtrust portal used for the management of the AeSign certificate requests, renewals, revocations, etc
LAWtrust Operations	the operational certificate support area of LAWtrust
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.

Item	Definition
Identity Documents for an Entity	Where the subscriber is a company or legal entity, the following must be used for the authentication and verification of a subscriber 1. a valid search done through Companies and Intellectual Property Commission (CIPC) or other accredited CIPC search provider or a Disclosure Certificate issued by CIPC, 2. power of attorney or letter of appointment by an authorised signatory of the company, close corporation, or other Entity, authorising a specific person to apply for or otherwise deal with LAWtrust in relation to the issuing, renewal or replacement of certificates, who will also be the key holder; and A copy of the identity document of any authorised key holder.
Identity documents for Natural persons	Where the subscriber is a natural person, the following documents must be used for the authentication and verification of a subscriber, ' 1. Identity document or Passport for initial registration Accredited certificate for Certificate renewal
Identity document	An identity document is used to verify aspects of a person's identity. Recognised identity documents for natural persons are; For South African citizens, 1. A valid and original "Green" Identity document or National ID Card issued by the South African Department of Home Affairs 2. A valid and original Passport issued by the South African Department of Home Affairs 3. A valid and original temporary identity document issued by the South African Department of Home Affairs For non-South African Nationals, a valid and original Passport issued by the applicant or subscribers country of origin Home Affairs department.
SCD	Private Cryptographic key stored in the SSCD under the 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.

Item	Definition
SKS	See Secure Key Store
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.
SSCD type 2	SSCD type 2 is in "EN14169-2 Protection Profile Secure signature creation device - Part 2: Device with import of key"

Table 1: Definitions and Acronyms

7. Public Key Infrastructure Configuration

7.1 Applicant and Subscriber

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

7.2 Eligibility for Certification

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

1. The applicant has a valid South African identity document or passport.
2. The applicant is in good standing with LAWtrust.
3. The applicant is fully aware of the responsibilities regarding the care and use of digital certificates and keys (as contained in the LAWtrust AeSign CPS, this Charter, the Advanced Electronic Signatures 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 e-mail.
2. Digital signing of documents and transactions.

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

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

The trust hierarchy is as follows:

- LAWtrust Root Certification Authority 2048 – Root Certification Authority (RCA)
- LAWtrust AeSign RA Charter – Local Certification and Issuing Authority (IA)
- LAWtrust AeSign-RA – Local Registration Authority (LRA)

The root key hierarchy is as follows:

- LAWtrust Root Certification Authority 2048 – ROOT CA
- LAWtrust LAWtrust AeSign CA(LAWtrust AeSign Certificates to be signed by this CA) – ISSUING CA

7.5 Certificate Type & Content

Certificate Type:

- X.509

Certificate Content:

- Email (applicant's email address)
- Common Name (Full Names & Surname)

- Company User ID (SerialNumber): optional
- Organisation Unit: LAWtrust AeSign RA
- Organisation: LAWtrust
- Country: ZA

7.6 Private Key Protection

The LAWtrust AeSign RA or LAWtrust appointed RA will issue LAWtrust AeSign 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.

7.6.1.1 Authentication of subscriber at generation of private key

The applicant's identity is verified prior to the point where the subscriber creates the SCCD password or when the subscriber provides the instruction to generate their private key.

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

The client has sole control for key generation since the client SSCD password is created by the user prior to the instruction of the user to generate the key.

7.6.1.2 Authentication scheme for accessing the private key

The LAWtrust Current authentication mechanism supported

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

2. Client SSCD: Token which the subscriber has possession of

Used together PIN and token are considered strong authentication.

7.6.1.3 Signature service authentication

The access to the signing keys is further enhanced by the authentication or the requester application to the signing application and or API. Is facilitated by using mutual authentication between the requesting application and the signing application and or API.

Combining the concepts in sections "7.6.1.1 Authentication of subscriber at generation of private key", "7.6.1.2 Authentication scheme for accessing the private key" and "7.6.1.3 Signature service authentication", enhances the security controls to achieve the highest levels of assurance of the user's sole control.

7.6.2 Client SSCD

The SafeNet eToken FIPS 140-2 cryptographic USB token is chosen as the client SSCD;

7.6.3 Supply of SSCD's

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

Client SSCD: FIPS 140-2 compliant Client SSCD for key generation and key storage

The appointed Enrolment Officers will perform the following SSCD personalization procedures before issuing a SSCD to an Applicant:

Personalise the SSCD with the provided security policy if required;

The appointed Enrolment Officer will perform the following steps in preparing the Applicant for a certificate download onto the client SSCD:

Install the SafeNet SAC client software on the Applicant's laptop/workstation;

Assist the Applicant in inserting the assigned client SSCD and ensure the Applicant changes the client SSCD PIN on first use.

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.

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 Application for a LAWtrust AeSign Digital Certificate

The LAWtrust AeSign RA shall be entitled to accept and process applications for entities and end entities\natural persons for the issue of a LAWtrust AeSign Certificate.

As a minimum the LAWtrust AeSign RA shall require from the natural person applicant:

- A duly completed and signed LAWtrust AeSign Subscriber Agreement authorised by the LAWtrust verification officer.
- A copy of the applicant's South African Identity Document or Passport.
- A FIPS 140-2 Secure Key Store issued and registered by LAWtrust.

The LAWtrust AeSign RA shall retain all of the documentation relevant to the authentication of the identity of the applicant as well as the verification of supporting information securely (LAWtrust PKI Safe), in conformance with the requirements of the LAWtrust Policy Authority, for a period of 7 (seven) years after the expiry or revocation of the LAWtrust AeSign Certificate.

8.2 Applicant Identity Verification

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

1. Perform a face-to-face verification 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 a fake (LAWtrust 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 LAWtrust Enrolment Officer).

4. Capture a photograph of the Applicant, including the face.

5. Collect the LAWtrust AeSign Subscriber Agreement and the copy of the identity document for storing with other LAWtrust AeSign application documentation in the LAWtrust File Safe.

8.3 Process of Certificate Request Verification

The LAWtrust AeSign RA appointed verification officer will perform the following steps to verify the certificate request:

1. Receive a LAWtrust Advanced Electronic Signature Certificate Subscriber Agreement that has been signed by the applicant.

2. Ensure that the South African Identity Document or Passport presented by the applicant is genuine.

3. Perform physical verification of the applicant's identity with face-to-face verification against the applicant's South African Identity Document or Passport.

4. Use best effort to verify the email address.

5. Authorise the certificate application (LAWtrust Advances Electronic Subscriber Agreement). Advising on the Outcome of the Application

An applicant who has applied for the issue of a LAWtrust AeSign Certificate will be referred to as a subscriber as described in section 7.1. The Subscriber shall be advised of the outcome of the issuance during the enrolment process.

8.4 Process of Secure Key Store Issuance and Registration

The LAWtrust AeSign RA appointed administrator will perform the following steps to personalize and register a Secure Key Store to an applicant:

8.4.1 For Cryptographic Tokens

1. Personalise the FIPS 140-2 crypto token via the SafeNet client software:
    a. Set the default token policy.
    b. Randomize the administrator's PUK (to be able to reset PIN)
    c. Set a default PIN.
    d. Set token to set new PIN on first use.
2. Register the FIPS 140-2 crypto token to the applicant:
    a. Record applicant's name
    b. Record applicant's surname
    c. Record applicant's unique ID (if applicable)
    d. Record applicant's mobile number
    e. Record applicant's detail in the token database.
3. Issue the token to the applicant and provide the token drivers required to use the token on the applicant's laptop/desktop.
4. The token administrator shall, if required by the applicant, provide assistance to the applicant in the installation of the token driver software on the applicant's laptop/desktop.

8.5 Process of user Enrolment

Online electronic enrolment will be done and the following enrolment fields are compulsory:

1. Common name (CN) (Full Names & Surname)
2. Email address (E)
3. Company User ID (Serial number - optional)

The LAWtrust AeSign RA appointed certificate administrator will perform the following steps to issue a certificate:

1. Receive a request (approved LAWtrust AeSign Subscriber Agreement Form).
2. Register the applicant and create the reference number and authorisation code on the LAWtrust AeSign Certificate Management System.
3. Deliver the reference number and authorisation code that will enable the download of the certificate to the applicant's Secure Key Store. The delivery may be performed in an out of band manner.

8.6 AeSign Certificate Issuance Process

Online electronic enrolment will be done and the following enrolment fields are compulsory:

1. Common name (CN) (Full Names & Surname or Entity Name)
2. Email address (E)
3. Company User ID (–Unique identifier {optional})

The LAWtrust AeSign RA appointed certificate administrator will perform the following steps to issue a certificate:

8.6.1 For Cryptographic Tokens

1. Receive a request (approved LAWtrust Advances Electronic Signature Subscriber Agreement Form).
2. Insert the token into the applicant's laptop/desktop – change the token PIN if it is the first-time usage.
3. Log on to the LAWtrust AeSign Enrolment Application (enrolment stations)
4. Enrol the applicant on the LAWtrust AeSign Enrolment Application and capture the following:
    a. User ID number;
    b. User full first names and last names;
    c. Email address;
    d. Mobile number;
    e. Scan ID document;
    f. Take picture of applicant;
    g. Request AeSign certificate.
5. Provide the subscriber the mechanism to enter the token PIN when requested.
6. The required keys will be generated and the AeSign certificate will be installed on the subscriber's token.
7. LAWtrust AeSign RA shall, if required by the applicant, provide telephonic assistance to the subscriber for the use of the LAWtrust AeSign Certificate.

8.6.2 Time to process certificate applications

8.6.2.1 Certificate Authority

The LAWtrust AeSign CA will process a CSR immediately on receiving such a request.

8.6.2.2 Registration Authority

The LAWtrust AeSign RA will process an application in line with the service level agreement between the RA and applicant or between the RA and the applicant's organisation service level agreement.

8.6.3 Proving possession of private key

In both cases a Certificate Signing Request signed by the applicant's private key will be generated and sent to the CA together with the public key. The CA will then verify the CSR using the public key. This is the mechanism used to prove that the applicant is in possession of the key pair.

8.7 Acceptance of Certificate

After the issuance of the LAWtrust AeSign Certificate to the subscriber, the subscriber shall check that the content of the LAWtrust AeSign Certificate is correct.

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

8.8 Advising on the Outcome of the Application

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

The LAWtrust AeSign RA will give verbal notice to the applicant of the refusal by the LAWtrust AeSign RA to issue an AeSign Certificate during the enrolment process if the AeSign requirements are not met.

The LAWtrust AeSign RA will notify the Applicant of the outcome of the application in person or via email using the email address recorded in the application.

8.9 Certificate use verification

- The certificate validity can be verified in the LAWtrust CRL [http://aesigncrl.lawtrust.co.za/CRL/lawtrust_aesign_ca_crlfile.crl].
- The CRL profile will be a full CRL.
- The certificate is valid for five years from date of issue.

9. Digital Certificate status changes

9.1 Rename user (change user CN)

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

9.2 LAWtrust AeSign Certificate Revocation and Suspension

9.2.1 Circumstances for revocation and suspension

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

LAWtrust AeSign Certificates may be revoked or suspended under 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 AeSign CA 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 AeSign CPS or the AeSign Subscriber Agreement entered into with the Subscriber;

7. Non-payment of fees in respect of any services provided by LAWtrust or LAWtrust AeSign RA.
8. Issue or use of the certificate not in accordance with the LAWtrust AeSign 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 AeSign CA or LAWtrust Root CA 2048 expires.
12. A determination by the LAWtrust AeSign CA or a LAWtrust AeSign RA that the certificate was not issued in accordance with this LAWtrust AeSign CPS or the provisions of the Subscriber's Agreement entered into with the Subscriber; or
13. Any other reason that the LAWtrust AeSign CA reasonably believes may affect the integrity, security, or trustworthiness of a LAWtrust Certificate.

9.2.2 LAWtrust AeSign Certificate Revocation Process

A request to revoke a LAWtrust AeSign Certificate may be submitted by a Subscriber, the LAWtrust AeSign RA, an Agent appointed by LAWtrust or the LAWtrust AeSign CA if any of the above occurs.

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

1. The LAWtrust Enrolment Officer will 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 three security question answers provided telephonically by Subscriber.
2. The LAWtrust Enrolment Officer will log on to the LAWtrust AeSign CA Administration Portal and issue a revocation request with the relevant revocation reason.

3. The LAWtrust AeSign CA shall within 24 hours of receiving a revocation request, post the serial number of the revoked LAWtrust AeSign Certificate to the CRL in the LAWtrust repository.

4. The LAWtrust AeSign RA shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust AeSign Certificate has been revoked.

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

9.3 LAWtrust AeSign Certificate Suspension

A request to suspend a LAWtrust AeSign Certificate may be submitted by the LAWtrust AeSign RA, an Agent appointed by LAWtrust or the LAWtrust AeSign CA if any of the revocation/suspension reasons occur.

The RA Enrolment Officer will perform the following steps to suspend the Subscriber LAWtrust AeSign Certificate:

1. The LAWtrust Enrolment Officer will log on to the LAWtrust AeSign CA Administration Portal and issue a suspension request with the relevant suspension reason.

2. The LAWtrust AeSign CA shall within 24 hours of receiving a suspension request, post the serial number of the suspended LAWtrust AeSign Certificate to the CRL in the LAWtrust repository.

3. The LAWtrust AeSign RA shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust AeSign Certificate has been suspended.

Suspension of a LAWtrust AeSign CA Certificate shall not affect any of the Subscriber's contractual obligations under the LAWtrust Advanced Electronic Signature Subscriber Agreement entered into by the Subscriber.

9.4 LAWtrust AeSign Certificate Re-Instatement

9.4.1.1 Circumstances for lifting certificate suspension

A certificate may be suspended if circumstances have arisen or are suspected and not yet verified, which may result in a revocation. If the evidence supporting the suspicion is later found to be invalid, then this would be grounds for lifting the suspension.

9.4.2 LAWtrust AeSign Certificate Re-Instatement process

A request to lift the suspension on a LAWtrust AeSign Certificate may be submitted by the LAWtrust AeSign RA, an Agent appointed by LAWtrust or the LAWtrust AeSign CA 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 LAWtrust AeSign Certificate:

1. The LAWtrust appointed Enrolment Officer will log on to the LAWtrust AeSign CA Administration Portal and issue an un-hold (lift suspension) request for the specific certificate.
2. The LAWtrust AeSign CA shall within 24 hours of receiving an un-hold request, remove the serial number of the suspended LAWtrust AeSign Certificate from the CRL and republish the CRL to the LAWtrust repository.
3. The LAWtrust appointed AeSign RA shall make a commercially reasonable effort to notify the Subscriber that the LAWtrust AeSign Certificate has been reinstated (un-suspended).

9.5 LAWtrust AeSign Certificate Renewal

9.5.1 Certificate Renewal Integrity checking

The CA and the RA shall maintain controls to provide reasonable assurance that certificate renewal requests are accurate, authorized and complete. The controls selected are included in the list below;

1. The certificate renewal request should include at least the subject's distinguished name, the serial number of the certificate and the expiry date of the current certificate.
2. The requesting legal entity digitally sign the certificate renewal request using the private key that relates to the public key contained in the requesting legal entity's existing public key.

3. The CA or the RA should process the certificate renewal data to verify the identity of the requesting legal entity and identify the certificate to be renewed.

9.5.2 Certificate renewal process

The LAWtrust AeSign Certificate will be renewed on the approach of the expiry date for the certificate. The renewal of web certificates will be managed by the subscribers and will require informing the LAWtrust AeSign RA of the upcoming expiry.

The LAWtrust AeSign RA will issue a new reference number and a new authorisation code for the subscriber account.

After the subscriber has provided the LAWtrust certificate administrator with a copy of their identity document to confirm the identity, the LAWtrust administrator will assist the subscriber onsite or remotely to download the new certificate from the LAWtrust AeSign enrolment pages. During this process the subscriber will be required to enter their Secure Key Store PIN for the new key pair to be generated and stored on the Secure Key Store.

During the certificate renewal the subscriber will undergo a re-key and the new public key information will be included in the new LAWtrust AeSign Certificate.

9.6 LAWtrust AeSign Certificate re-key

In the case where there is a certificate re-key required, the following verification process will be followed.

1. Verify applicant Full Names and Surname (check is the ID versus the name in the organisation email signature. The least first name and surname should correspond, second and third names may not appear in the email signature.

The subscriber email address will be verified as per section 8.3.

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 client SSCD

10.2 Life cycle management of the SSCD.

10.2.1 Client SSCD

Client SSCD requirements are in conformance to FIPS 140-2. The client SSCD lifecycle can be described as follows

1. SSCDs are ordered from a LAWtrust approved supplier.
2. SSCDs are pre-initialised with the LAWtrust configuration
3. Pre-initialised SSCDs are provided to enrolment officers to issue to subscribers.
4. SSCDs are issued to subscribers, at the same time that the digital certificate requirement for face-to-face identity verification is performed.
5. SSCDs and the digital certificate which resides within the SSCD are used by the subscriber
6. If a SSCD is lost or stolen or compromised, the certificate is revoked and new SSCD and certificate is issued.
7. If subscribers have a change in job status, which does not require the use of the certificate, the certificate is revoked, the SSCD is recycled (wiped clean\re-initialised) and reissued to another subscriber.

10.3 LAWtrust AeSign SSCD PIN Reset

1. If a LAWtrust AeSign Certificate Subscriber forgets their PIN to access the SafeNet eToken, then the following process will be followed to reset the PIN:The

LAWtrust Enrolment Officer will perform the following identity verification for the Subscriber:

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

b. Verify three security question answers provided telephonically by Subscriber.

2. For eToken PIN reset the LAWtrust Enrolment Officer will:

a. Request the Subscriber to provide their eToken serial number.

b. Retrieve the Subscriber's eToken PUK from the LAWtrust database.

c. Assist the Subscriber onsite or remotely via a TeamViever session to reset their token PIN following the SafeNet eToken PIN reset guide.

11. LAWtrust AeSign RA Annual Audit

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

12. References

Reference	Details
CA Policies, Practices & Agreements:	LAWtrust AeSign CA Certificate Practices Statement (https://www.lawtrust.co.za/repository). LAWtrust Advanced Electronic 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
Guidelines	SafeNet eTokens personalization guide SafeNet eToken PIN reset guide

13. Sign Off Acceptance

Name:	Bruce Anderson
Authority:	Policy Authority
Title:	Chief Information Security Officer
Date:	2017-10-30
Signature:	Signed by: Bruce Anderson Signed at: 2017-10-30 11:44:29 +02:00 Reason: I approve this document