	INFORMATION SECURITY POLICY
	ISSUE SPECIFIC POLICY
	VERSION: 13-03-2007
	EFFECTIVE DATE: 01-03-2007

# Certification Practice Statement

---


## **Law Trusted Third Party Services (Pty) Ltd**

registration number 2001/004386/07  
("L@Wtrust")

Unit 6 Central Park, 13 Esdoring Street,  
Highveld Technopark , Centurion,  
Pretoria, South Africa

Phone +27 (0)12 676 9243 • Fax +27 (0)12 665 3997  
Web [www.lawtrust.co.za](http://www.lawtrust.co.za) • Email [governance@lawtrust.co.za](mailto:governance@lawtrust.co.za)

*L@Wtrust reserves the right to change or amend this certification practice statement at any time without prior notice. Changes will be posted on the L@Wtrust website [www.lawtrust.co.za/repository] from time to time. If you have any queries about this document please contact L@Wtrust.*

	Classification	LEVEL 1 Public information
	Reference	LT_ISP_IS_CP_01.doc
	Location	<a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a>
	Version	13-02-2007
	Policy Authority	L@Wtrust PA

**COPYRIGHT NOTICE**

**L@WTRUST (PTY) LTD (“L@WTRUST”) RETAINS THE COPYRIGHT IN THIS CERTIFICATION PRACTICE STATEMENT (“CPS”) AS WELL AS ANY NEW VERSIONS OF IT PUBLISHED AT ANY TIME BY L@WTRUST.**

**L@WTRUST FURTHER RETAINS THE COPYRIGHT IN ALL DOCUMENTS PUBLISHED OR APPROVED THE L@WTRUST POLICY AUTHORITY (“L@WTRUST PA) UNDER AND IN TERMS OF THE PROVISIONS OF THIS CPS.**

**THE COPYING OR DISTRIBUTION OF THIS CPS OR DOCUMENTS APPROVED BY THE L@WTRUST PA, IN WHOLE OR IN PART, AND CONTRARY TO THE PROVISIONS OF 0 OF THIS CPS WITHOUT THE PRIOR WRITTEN CONSENT OF THE L@WTRUST PA, IS STRICTLY PROHIBITED.**

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## TABLE OF CONTENTS

1.	Introduction .....	4
2.	PUBLICATION AND REPOSITORY RESPONSIBILITIES .....	17
3.	IDENTIFICATION AND AUTHENTICATION .....	20
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	26
5.	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	38
6.	TECHNICAL SECURITY CONTROLS.....	44
7.	CERTIFICATE PROFILES.....	47
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....	48
9.	OTHER BUSINESS AND LEGAL MATTERS .....	50

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 1. Introduction

### 1.1 Overview

This document is the Certification Practice Statement (CPS) of the L@Wtrust Certification Authority (L@Wtrust CA).

This CPS describes the certification practices that have been implemented to ensure the L@Wtrust CA trustworthiness in issuing public key certificates to subscribers. It has been drafted to satisfy the requirements of the L@Wtrust CA Certificate Policy (CP) for issuing L@Wtrust Certificates.

This CPS is intended to allow participants to the L@Wtrust public key infrastructure (PKI) to assess the trustworthiness of the L@Wtrust CA and determine suitability of L@Wtrust Certificates in meeting the requirements in the communication of electronic information.

This CPS also prescribes the practices and procedures which the L@Wtrust CA will require of all Registration Authorities (L@Wtrust RA's) operating under its authority as well as the rights and obligations of third parties including, but not limited to, applicants, subscribers and relying parties.

### 1.2 Document name and identification

This document title is L@Wtrust Certification Practice Statement. You may consider the version of the L@Wtrust CPS available for download from the L@Wtrust website [[www.lawtrust.co.za/repository](http://www.lawtrust.co.za/repository)] as the most current version as at the time of downloading.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 1.3 PKI participants

### 1.3.1 L@Wtrust CA

The L@Wtrust CA is chained into the Public hierarchy of the Entrust.net root Certificate Authority. This offers certificates with the following hierarchy

Entrust.net Secure Server Certification Authority

↳LAWtrust Certification Authority

↳Subscriber

The L@Wtrust CA may:

- accept the Certificate Signing Requests (“CSR”) with the public keys of an applicant from a L@Wtrust RA which has authenticated the identity and verified information to be contained in the L@Wtrust Certificate applied for by the applicant;
- once the CSR is verified the L@Wtrust CA will create a L@Wtrust Certificate containing the public key;

A L@Wtrust Certificate created in response to the CSR will be digitally signed by the L@Wtrust CA.

### 1.3.2 Registration authorities

The L@Wtrust CA may authorise representatives or agents, including L@Wtrust RA’s to:

- accept applications for a L@Wtrust Certificate;
- perform authentication of identities and verification of information submitted by applicants when applying for a L@Wtrust Certificate in terms of a L@Wtrust RA Charter approved by the L@Wtrust Policy Authority (L@Wtrust

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

PA); where such authentication and verification is successful, submit the CSR to the L@Wtrust CA, in accordance with the provisions of this CPS.

### **1.3.3 Applicants**

An applicant is a person, entity, or organisation that has applied for but has not yet been issued a L@Wtrust Certificate.

### **1.3.4 Subscribers**

A subscriber is a person, entity, or organisation that has been issued a L@Wtrust Certificate.

### **1.3.5 Relying parties**

A relying party is a person, entity, or organisation that relies on or uses a L@Wtrust Certificate and/or any other information provided in the L@Wtrust repository to verify the identity and public key of a subscriber and/or use such public key to send or receive encrypted communications to or from a subscriber.

### **1.3.6 Other participants**

Other participants are entities within South Africa on whom L@Wtrust will rely in verifying information relating to an applicant for issuing a L@Wtrust Certificate.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 1.4 Certificate usage

The L@Wtrust CA is capable of manufacturing two certificate types; managed or enterprise certificates and unmanaged or web certificates. The significant difference being that key recovery is available for managed certificates, the functionality of signing and encryption is the same for both certificates. The specifics of the certificate to be used will be defined in a Registration Authority Workshop.

### 1.4.1 Prohibited certificate uses

Any use falling outside the L@Wtrust Certificate uses described in this CPS shall be deemed to be a prohibited use.

L@Wtrust Certificates are not designed or intended for use in or in conjunction with hazardous activities or uses requiring failsafe performance and the use of the certificates in this regard is strictly prohibited.

### 1.4.2 Appropriate certificate uses

L@Wtrust Certificates may be used for the following purposes:

- Authenticate the identity of the subscriber;
- To encrypt electronic communications sent by the subscriber;
- To decrypt electronic communications received by a subscriber;
- To digitally sign electronic communications.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 1.5 Policy administration

### 1.5.1 Security Management

Governed by the L@Wtrust Information Security Management Program, L@Wtrust has structured the Policy documentation in the following manner;

Enterprise Security Polices; (Including Data Sensitivity, Security Management, System Integrity, Personnel Integrity, Hardware Integrity, Configuration Management (CM))

System Specific Policies; (Including Networks, Gateways/Firewalls, Smart Cards/Tokens, Administrator Workstations, etc...)

Issue Specific Polices; (Including Certificate Policy, Certificate Practice Statement, etc...)

### 1.5.2 Roles and responsibilities

In order to ensure universal adoption of the Policies L@Wtrust has set up two authority bodies comprising of senior management membership. The L@Wtrust Policy Authority (L@Wtrust PA) shall be responsible for all Policy administration; such policies include the L@Wtrust CP. The L@Wtrust Operating Authority (LAWTrust OA) is the body responsible for the CPS administration and implementation, this includes all procedures and standards required to ensure correct implementation of the CPS. The CPS is based on the policies established by the L@Wtrust PA.



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### 1.5.3 Organisation administering the document

The L@Wtrust PA shall administer all the Security Policies within the L@Wtrust Information Security Management Program, this includes the L@Wtrust CP, CPS and L@Wtrust RA Charters.. The L@Wtrust OA shall be responsible for the implementation of the CPS and related procedures.

### 1.5.4 Person determining CPS suitability for the policy

The L@Wtrust PA shall determine suitability for the Policy.

### 1.5.5 CPS approval procedures

The CPS is developed by the L@Wtrust PA and the L@Wtrust OA.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 1.6 Definitions

asymmetric cryptosystem	See definition of cryptography
authenticate/ authentication	<p>Authentication: verification of an individuals claimed identity:</p> <p>a) at registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity;</p> <p>b) during use, the act of comparing electronically submitted identity and credentials (i.e. user ID and password) with stored values to prove identity.</p>
CA	See definition of certificate authority.
certificate administrator	A trusted individual that performs certain trusted tasks (e.g. authentication) on behalf of a CA or RA. This person is usually a member of the personnel of such CA or RA.
certificate	See definition of digital certificate.
certificate/certification authority	A legal entity that issues, signs, manages, revokes and renews digital certificates.
certificate policy	A named set of rules that indicate the applicability of a digital certificate to a particular community and or class of application with common security requirements. The practices required to give effect to the rules set out in the certificate policy are set out in the certification practice statement.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

CP	See definition of certificate policy.
CPS	See definition of certification practice statement.
certification practice statement	In order to comply with the rules set out in the certificate policy, the CPS details the practices that a certificate authority needs to employ when issuing, managing, revoking, renewing, and providing access to digital certificates, and further includes the terms and conditions under which the certificate authority makes such services available.
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. 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.
cryptography services.	A service provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of a digital certificate/digital signature scheme for the purpose of ensuring (i) that data or data messages can be accessed or can be put into an intelligible form only by certain persons, (ii) that the authenticity or integrity of such data or data message is capable of being ascertained, (iii) the integrity of the data or data message, or (iv) that the source of the data or data message can be correctly ascertained.
data	Electronic representations of information in any form.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

data message	Data generated, sent, received or stored by electronic means.
digital certificate	A digitally-signed data message that is a public-key certificate in the version 3 format specified by ITU-T Recommendation X.509, which includes the following information: (i) identity of the Certificate Authority issuing it; (ii) the name or identity of its subscriber, or a device or electronic agent under the control of the subscriber; (iii) a Public Key that corresponds to a Private Key under the control of the subscriber; (iv) the validity period; (v) the Digital Signature created using a private Key of the certificate authority issuing it; and (vi) a serial number.
digital signature	A transformation of a data message using an asymmetric cryptosystem such that a person having the initial data message and the signer's public key can determine whether: (i) the transformation was created using the private key that corresponds to the subscriber's public key; and (ii) the message has been altered since the transformation was made.
digital signature validation	In conjunction with the public key component of the correct public/private key pair, the signature of a data object can be verified by: <ol style="list-style-type: none"> <li>1. decrypting the signature object with the public key component to expose the original hash value,</li> <li>2. re-computing a hash value over the data object, and</li> <li>3. comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.</li> </ol>

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

digitally sign	<p>The act of generating a digital signature for a data message, which is created by:</p> <ol style="list-style-type: none"> <li>1. Hashing the object to be signed with a one-way hash function; and</li> <li>2. Encrypting (signing) the hash value with the private key component of a key pair.</li> </ol> <p>The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.</p>
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.
e-mail	Electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

integrity	Integrity is a cryptography service that ensures that modifications to data are detectable.
key pair	Two mathematically related cryptographic keys, referred to as a private key and a public key, having the properties that (i) one key (the public key) can encrypt a message which only the other key (the private key) can decrypt, and (ii) even knowing the one key (the public key), it is computationally infeasible to discover the other key (the private key).
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.
non-repudiation	The concept of ensuring that an action cannot later be denied by any of the parties involved.
PKI	See definition of public key infrastructure.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

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.
private key	The key of a key pair used to create a digital signature and is required to be kept secret.
public key	The key of a Key Pair used to verify a Digital Signature and may be publicly disclosed.
RA	See definition of registration authority.
registration authority	An entity that: (i) receives certificate applications, and (ii) validates information supplied in support of a certificate application, (iii) requests a certificate authority to issue a certificate containing the information as validated by the registration authority, and (iv) requests a certificate authority to revoke certificates issued;
Relying Party	A person that relies on a certificate or other data that has been digitally signed.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

relying party agreement	An agreement between the certificate authority and a relying party that sets out the terms and conditions governing reliance upon a certificate or data that has been digitally signed
signature	Any mark made by a person that evidence's that person's intention to bind himself/herself to the contents of a document to which that mark has been appended. Depending on the circumstances, this could be a handwritten signature or a digital signature.
subscriber	an applicant whose Certificate Application has been approved, and has been issued a certificate, and who is the subject named or otherwise identified in the certificate, controls the private key that corresponds to the public key listed in that certificate, and is the individual to whom digitally signed data messages verified by reference to such certificate are to be attributed.
subscriber agreement	An agreement between the certificate authority and a subscriber that sets out the terms and conditions governing the issuance of a certificate, control of the private key that corresponds to the public key listed in the certificate, acceptable use of the certificate, notification of compromise of the private key, and matters ancillary and related thereto.



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 Repositories

The L@Wtrust CA maintains the L@Wtrust repositories to allow access to L@Wtrust Certificate Authority related information. The repositories host general CA documentation, certificate status information and any further information which may from time to time be required by the L@Wtrust PA. There are two categories of repositories;

#### 2.1.1 Document repository:

The document repository hosts the policies and general CA documentation. Examples of the documents found in this repository include:

- the L@Wtrust CP,
- the L@Wtrust CPS,
- the L@Wtrust RA Charters,
- information and agreements relating to the subscription for and reliance on L@Wtrust Certificates;
- and any further information which may from time to time be required by the L@Wtrust PA.

The information in the document repository is accessible through a web-interface [<https://www.l@wtrust.co.za/repository>] and is periodically updated in terms of this CPS.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### 2.1.2 Certificate status repository

The certificate status is published in two formats.

- **CRL 1(web interface access):**

The L@Wtrust certificate revocation list (CRL) accessible through the web-interface (<http://crl.l@wtrust.co.za>) and is periodically updated in terms of this CPS.

- **CRL 2(light weight directory access protocol (ldap) access):**

The L@Wtrust certificate revocation list (CRL) accessible through the ldap interface

[<ldap://ldap.lawtrust.co.za:389/cn=CRL1,cn=LAWtrust,CA,o=LAWtrust,c=ZA>] and is periodically updated in terms of this CPS.

## 2.2 Publication of the CPS

This CPS is available from L@Wtrust in hardcopy upon request. This CPS published in the L@Wtrust repository shall be available by web-interface (<https://www.l@wtrust.co.za/repository>) at all times subject to any interruption of the L@Wtrust website services.

Changes or modifications to this CPS shall be published in accordance with directions given by the L@Wtrust PA.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### 2.3 Time or frequency of CPS publication

After acceptance by the L@Wtrust PA this CPS shall be published in the manner described in 2.2.

This CPS shall be reviewed as may be required due to:

- changes in existing practice, the introduction of new practices, changes in legislation or regulation governing the use of digital certificates or electronic signatures; or
- changes in the PKI within which the L@Wtrust CA provides certificates.

Changes shall be documented in revised versions of this CPS and become effective on the dates indicated in the revised CPS.

### 2.4 Access controls on repositories

This CPS and all other documents published in the L@Wtrust Repository will be available to all applicants, subscribers and relying parties, but may only be modified by the L@Wtrust PA.

	<b>Classification</b>	LEVEL 1 Public information
	<b>Reference</b>	LT_ISP_IS_CP_01.doc
	<b>Location</b>	<a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a>
	<b>Version</b>	13-02-2007
	<b>Policy Authority</b>	L@Wtrust PA

### 3. IDENTIFICATION AND AUTHENTICATION

Before issuing a certificate a L@Wtrust RA shall authenticate the identity and/or attributes of an applicant to be published in a L@Wtrust Certificate. This section of this CPS establishes the criteria for an acceptable application for a L@Wtrust Certificate and for the authentication of persons requesting the revocation of a L@Wtrust Certificate.

#### 3.1 Naming

##### 3.1.1 Types of names

A L@Wtrust Certificate shall include a common name component as required in the X501 Standard. The common name shall be the name most usually associated with the person or entity to whom a L@Wtrust Certificate is to be issued.

##### 3.1.2 Need for names to be meaningful

- **Naming Subscribers for Personal Certificates:**

The value of the common name attribute used in naming subscribers is the name indicated in an original, generally acceptable form of photographic identification, including but not limited to an identity document, passport or drivers licence.

- **Naming Subscribers for Entity Certificates:**

The value of the common name attribute used in naming subscribers for entity Certificates is the name, in the case of any entity that requires registration, under which the entity is registered and, in the case of an entity

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

not requiring registration, the name under which the entity conducts its activities.

### 3.1.3 Anonymity or pseudonymity of subscribers

L@Wtrust shall not provide anonymous certificates or certificates to individuals under a pseudonym.

### 3.1.4 Rules for interpreting various name forms

In the provision of personal certificates the names and identity number of persons will provide a unique name.

In those instances where the person has not had an identity number allocated to him or her, the date of birth (in numeric form) will be used instead of an identity number. In those instances where the names and date of birth in numeric form may conflict, a dispute as to the name of the subscriber shall be resolved by a person/s appointed by the L@Wtrust PA.

### 3.1.5 Uniqueness of names

- **Personal Identities**

The combination of the names, identity number or date of birth in numeric form, as the case may be, of the subscriber, together with the serial number attributed to the Certificate provides a unique electronic identity for the person associated with the certificate. L@Wtrust shall not re-use a serial number in respect of a L@Wtrust Certificate.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

- **Entity Identities**

The combination of the name and registration number together with the serial number attributed to the Certificate provides a unique electronic identity for the entity associated with the Certificate. L@Wtrust shall not re-use a serial number in respect of a L@Wtrust Certificate.

### 3.1.6 Recognition, authentication, and role of trademarks

The L@Wtrust CA may use registered trademarks when assigning the distinguished names to entities.

## 3.2 Initial identity validation

### 3.2.1 Method to prove possession of private key

The method of proving possession of a private key shall be authorised by the L@Wtrust CA and stated in the Registration Charter of a L@Wtrust RA.

In all instances in which the Charter of a L@Wtrust RA does not specifically provide for proof of possession of the private key, the onus of proving possession of the private key shall fall on the subscriber.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### 3.2.2 Authentication of personal identity

The L@Wtrust RA shall establish reasonable proof of identity of the person depending on the use that the Certificate is to be applied. The Charter of the L@Wtrust RA shall stipulate the information required for authentication of the identity and the method of verification of the information and shall be approved by the L@Wtrust PA.

### 3.2.3 Authentication of entity identity


The L@Wtrust RA shall reasonable establish proof of identity of the entity depending on the use that the Certificate is to be applied. The Charter of the L@Wtrust RA shall stipulate the information required for authentication of the identity and the method of verification of the information and shall be approved by the L@Wtrust PA.

### 3.2.4 Non-verified subscriber information

Certain information gathered for the purpose of certification may not be verified by a L@Wtrust RA provided that the information published in a L@Wtrust Certificate shall be verified as stipulated by the L@Wtrust PA.

### 3.2.5 Validation of authority

The L@wtrust CA is the authority to which any RA's under the L@Wtrust CA has been created. As such all rights, entitlements or permissions of subscribers within a specific organisation RA will be specified within the specific organisation RA charter.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### 3.2.6 Criteria for interoperation

Suitability and criteria for interoperation will be jointly determined by the L@Wtrust PA and the L@Wtrust OA. Where appropriate, Entrust will be included in such proposals.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

A L@Wtrust RA shall establish proof of identity of the person or entity and authenticate the identity of the applicant and verify the accuracy of information to be published in a L@Wtrust Certificate subject to a routine re-key in the manner determined in a L@Wtrust RA Charter. The stringency of authentication of identity and verification of information shall be commensurate with the minimum stipulations of the L@Wtrust PA for the certification required.


### 3.3.2 Identification and authentication for re-key after revocation

The L@Wtrust CA shall not renew L@Wtrust Certificates that have been revoked;

A subscriber who wishes to use a L@Wtrust Certificate after revocation must apply for a new L@Wtrust Certificate to replace the L@Wtrust Certificate that has been revoked;

A subscriber shall be required to complete a new application process as described in 3.2 including generation of a new key-pair and submission of all information required for an initial application for a L@Wtrust Certificate;



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

On revocation of a L@Wtrust Certificate the subscriber shall immediately cease using such a L@Wtrust Certificate and remove the L@Wtrust Certificate from any devices and/or software in which it has been installed.

### **3.4 Identification and authentication for revocation request**

A L@Wtrust RA shall provide for the manner in which authentication of the identity of any person requesting revocation of a certificate is established. These provisions will be contained in a L@Wtrust RA Charter which shall be approved by the L@Wtrust PA.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

#### 4.1.1 Who can submit a certificate application

An applicant or an applicant's manager may submit a certificate application.

L@Wtrust shall, under this CPS, issue:

- L@Wtrust Certificates in respect of natural persons.
- L@Wtrust Certificates in respect of recognised legal entities.

#### 4.1.2 Enrolment process and responsibilities

Applicants shall:

- complete and submit to a L@Wtrust RA an application for a L@Wtrust Certificate providing all information requested, without any errors, misrepresentations or omissions;
- in making the application, agree to be bound by the terms of this CPS and the applicable Subscriber Agreement;
- make payment to the L@Wtrust CA and/or L@Wtrust RA of all fees and charges in respect of the application for the issue of a L@Wtrust Certificate.

On receipt of a properly completed application, a L@Wtrust RA shall process the application and verify the information provided in terms of 3.2.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

If the application or information provided to the L@Wtrust RA is deficient, the L@Wtrust RA shall, at its discretion:

- use commercially reasonable efforts to notify the applicant by eMail at the eMail address provided for in the application, of the deficiency and of the refusal of the application;
- if the verification of the information submitted to the L@Wtrust RA is successful, the L@Wtrust RA shall submit a CSR to the L@Wtrust CA;
- notify the applicant, at the eMail address provided in the application, that the CSR has been submitted to the L@Wtrust CA and of the URL from which the applicant may retrieve the L@Wtrust Certificate when issued;

After the issue of the L@Wtrust Certificate neither the L@Wtrust CA or any L@Wtrust RA will have any obligation to perform any ongoing monitoring, investigation or verification of the information provided in the Certificate Application.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

The L@Wtrust CA shall process an application for the issue of a L@Wtrust Certificate only after a L@Wtrust RA has performed the authentication and verification checks provided for in the relevant L@Wtrust RA Charter.

Once the authentication and verification process has been completed the L@Wtrust RA shall provide all relevant information and confirmation of the authentication or verification to the L@Wtrust RA required by the L@Wtrust CA together with the CSR.

### 4.2.2 Approval or rejection of certificate applications

Approval of a certificate application will result in the process continuing. Application rejection will result in notification to the application the reason for the rejection.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### **4.2.3 Time to process certificate applications**

Any application for a certificate should be processed within 24 hours of receiving such a request.

### **4.3 Certificate issuance**

#### **4.3.1 CA actions during certificate issuance**

After satisfying itself that the information provided to it by a L@Wtrust RA is accurate and that the authentication and verification checks required by the L@Wtrust PA have been executed, the L@Wtrust CA may generate and digitally sign the L@Wtrust Certificate applied for in accordance with the certificate profile described in 7.1 of this CPS.

#### **4.3.2 Notification to subscriber by the CA of issuance of certificate**

Post issuance of the certificate the L@Wtrust CA shall make reasonable efforts to send an email to the subscriber (at the email address provided in the certificate application), stating the status of the issuance process.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

After issue of the L@Wtrust Certificate and notification addressed to the subscriber the subscriber shall check that the content of the L@Wtrust Certificate is correct.

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

By using the L@Wtrust Certificate in any manner contemplated in this CPS, the subscriber accepts the accuracy of the information contained in the L@Wtrust Certificate.

If the L@Wtrust CA is notified of any inaccuracies in the L@Wtrust Certificate by the subscriber the L@Wtrust Certificate shall be revoked in terms of the provisions of 4.9 of this CPS.

### 4.4.2 Publication of the certificate by the CA

Post issuance the certificate is published in the L@Wtrust CA ldap directory.

### 4.4.3 Notification of certificate issuance by the CA to other entities

There or no further communications to other entities.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

The subscriber shall only use the private key associated with the Certificate after the issue of the Certificate and shall not use the private key associated with the Certificate after the revocation or expiry of the L@Wtrust Certificate.


The subscriber shall use his/her/its private key and the L@Wtrust Certificate in strict compliance with the Subscriber Agreement entered into between the subscriber and L@Wtrust and this CPS.

### 4.5.2 Relying party public key and certificate usage

Relying parties shall comply strictly with the provisions of the Relying Party Agreement entered into between the relying party and L@Wtrust and shall be responsible for checking the status of any L@Wtrust Certificate before relying on the Certificate.

## 4.6 Certificate renewal

L@Wtrust Certificates may be renewed provided that the L@Wtrust RA conducts and confirms that it has conducted the necessary authentication and verification checks for the purposes of the Certificate renewal in accordance with the L@Wtrust RA Charter approved by the L@Wtrust PA.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### 4.7 Certificate re-key

The L@Wtrust CA shall not re-key certificates.

#### 4.8 Certificate modification


The L@Wtrust CA shall not modify certificates.

#### 4.9 Certificate revocation and suspension

The L@Wtrust CA shall revoke a L@Wtrust Certificate after receiving a valid revocation request from any L@Wtrust RA.

A L@Wtrust RA shall be entitled to request revocation of and shall request revocation of, and the L@Wtrust CA shall be entitled to revoke and may revoke subscriber's L@Wtrust Certificates if the L@Wtrust RA or L@Wtrust CA acquires knowledge of or has a reasonable basis for believing that any of the following events has occurred:

- the compromise of the L@Wtrust CA private key, or if applicable, the compromise of a superior Certification Authority's private key;
- breach by the subscriber of any of the terms of this CPS or the Subscriber Agreement entered into with the subscriber;
- any change in the information contained in the L@Wtrust Certificate issued to a subscriber;
- non-payment to L@Wtrust of any L@Wtrust Certificate fees or service fees by the subscriber;

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

- a determination by the L@Wtrust CA or a L@Wtrust RA that the Certificate was not issued in accordance with this CPS or the provisions of the Subscriber's Agreement entered into with the subscriber; or
- any other reason that the L@Wtrust CA reasonably believes may affect the integrity, security, or trustworthiness of a L@Wtrust Certificate.

#### **4.9.1 Circumstances for revocation**

A subscriber shall request revocation of a L@Wtrust Certificate if the subscriber has a suspicion or knowledge of a compromise of the subscriber's private key or that the information contained in L@Wtrust Certificate has become inaccurate, incomplete, or misleading as a result of change in circumstances relating to the subscriber.

A request for revocation by a subscriber shall be submitted to a L@Wtrust RA and processed with the subscriber's application for a new L@Wtrust Certificate (if applicable).

Revocation of a L@Wtrust Certificate shall not affect any of the subscriber's contractual obligations under this CPS or the Subscriber's Agreement entered into by the subscriber or any relying party agreements.

#### **4.9.2 Who can request revocation**

A subscriber may request revocation of his/her/its L@Wtrust Certificate at any time and for any reason.

The L@Wtrust CA or L@Wtrust RA may request revocation of a L@Wtrust Certificate if it reasonably believes that the L@Wtrust Certificate or public key associated with the L@Wtrust Certificate has been compromised.

Before revoking a Certificate at the request of a subscriber the L@Wtrust CA shall use commercially reasonable efforts to validate the identity of the subscriber or the person representing the subscriber and shall not be required to revoke the L@Wtrust



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

Certificate until it is satisfied as to the identity of the subscriber. The subscriber shall comply with any reasonable requests of the L@Wtrust CA relating to validating the identity of the subscriber making a revocation request.

#### 4.9.3 Procedure for revocation request

A L@Wtrust RA shall authenticate a request by a subscriber for revocation of he/she/its L@Wtrust Certificate by requiring:

- a sub-set of the information provided by the subscriber with the subscriber's L@Wtrust Certificate application; or
- the pass-phrase submitted by the subscriber with the subscriber's L@Wtrust Certificate application; or
- verification by an authorised contact at the entity to which or under which the L@Wtrust Certificate has been issued;
- on receipt of confirmation of the information required in 4.0.5.0 a L@Wtrust RA shall send a revocation request to the L@Wtrust CA;
- the L@Wtrust CA receiving the revocation request shall, within 48 hours of receiving such revocation, post the serial number of the revoked L@Wtrust Certificate to the CRL in the L@Wtrust repository (<http://crl.lawtrust.co.za>);
- if a subscriber's L@Wtrust Certificate is revoked for any reason, the L@Wtrust RA that requested revocation of the subscribers L@Wtrust certificate shall make a commercially reasonable effort to notify the subscriber by sending an eMail to the eMail address provided in the Certificate application.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### **4.9.4 Revocation request grace period**

In the case of a private key compromise or suspected private key compromise, the subscriber shall request revocation of the associated L@Wtrust Certificate immediately upon detection of the compromise or suspected compromise.

Revocation requests for other required reasons shall be made as soon as reasonably practicable.

#### **4.9.5 Time within which CA must process the revocation request**

The L@Wtrust CA shall use commercially reasonable efforts to issue CRL's at least once every 24 hours. CRL's will generally be issued at approximately 12h00 South African Standard Time. In certain circumstances CRL's may also be issued between these intervals, such as in the event of detection of a serious compromise.

#### **4.9.6 Revocation checking requirement for relying parties**

Relying parties shall check CRL's on a daily basis to ensure reliance on L@Wtrust Certificates.

#### **4.9.7 On-line revocation/status checking availability**

A Relying party shall check whether the L@Wtrust Certificate that the relying party wishes to rely on has been revoked. A relying party shall check the CRL's maintained in the appropriate repository to determine whether the L@Wtrust certificate that the relying party wishes to rely on has been revoked. In no event shall L@Wtrust or any registration authority operating under the L@Wtrust CA, or any sub-contractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable for any damages whatsoever due to:

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

- The failure of a relying party to check the revocation or expiry of a L@Wtrust Certificate; or
- Any reliance by a relying party on a L@Wtrust Certificate that has been revoked or that has expired.

#### **4.9.8 On-line revocation checking requirements**

No stipulation.

#### **4.9.9 Other forms of revocation advertisements available**

The CRL's in the L@Wtrust repository may be searched by serial number. No other mechanisms are provided.

#### **4.9.10 Special requirements re key compromise**

If a subscriber suspects or knows that a private key corresponding with the public key contained in the subscriber's L@Wtrust Certificate has been compromised, the subscriber shall immediately notify the L@Wtrust RA that processed the subscriber's L@Wtrust Certificate application using the procedures set out in 4.9.3, of such suspected or actual compromise.

The subscriber shall immediately stop using the L@Wtrust Certificate and shall remove such L@Wtrust Certificate from any devices and/or software on which the L@Wtrust Certificate has been installed;

The subscriber shall be responsible for investigating the circumstances of such compromise or suspected compromise and for notifying the L@Wtrust CA and any relying parties that may have been affected by such compromise or suspected compromise.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### **4.9.11 Circumstances for suspension**

A L@Wtrust RA may suspend a L@Wtrust Certificate if the subscriber is not in good standing with the L@Wtrust CA or the L@Wtrust RA or the subscriber fails to adhere to the provisions of this CPS or the L@Wtrust RA's Charter.

#### **4.9.12 Who can request suspension**

A L@Wtrust RA may request a L@Wtrust CA to suspend a L@Wtrust Certificate without notice to the subscriber. The L@Wtrust RA shall make a commercially reasonable effort to notify the subscriber of the suspension by sending an eMail to the eMail address provided in the Certificate Application.

#### **4.9.13 Procedure for suspension request**

A L@Wtrust RA may request a L@Wtrust CA to suspend a L@Wtrust Certificate in accordance with the provision of the relevant L@Wtrust RA Charter as approved by the L@Wtrust PA.


#### **4.9.14 Limits on suspension period**

A L@Wtrust RA may suspend a L@Wtrust certificate for a period not exceeding the validity of the L@Wtrust certificate.

### **4.10 Certificate status services**

The L@Wtrust CA shall maintain a CRL with a validity of 24 (twenty four) hours.

The L@Wtrust CA shall reissue CRL's from time to time to ensure the availability of service for parties relying on the CRL.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### 4.11 Key escrow and recovery policy and practices

The L@Wtrust CA may provide a key escrow service under the control of the relevant L@Wtrust RA for those subscribers requiring key escrow.

A L@Wtrust RA may provide key escrow services in accordance with the provisions of the L@Wtrust RA Charter governing the provision of such services as may be approved by the L@Wtrust PA.

Keys shall only be recovered for purposes of disaster recovery and immediately they are no longer required for this purpose shall be revoked save in the instance of L@Wtrust Certificates which provide encryption only.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

### 5.1 Physical controls

Entrust software (Security Manager) is used as the software component of the L@Wtrust CA. The hardware and software for the L@Wtrust CA is located in a secure facility with physical security and access control procedures that meet or exceed industry standards.

#### 5.1.1 Site location and construction

The L@Wtrust CA is hosted in a high security vault at Internet Solutions Data Centre in Rosebank, Johannesburg.

#### 5.1.2 Physical access

Physical access to the L@Wtrust CA is strictly and biometrically controlled. Only authorised L@Wtrust representatives may arrange to gain access to the Internet Solutions Data Centre and they and all persons accompanying them under their authority are identified by reference to a document containing a photographic image of the person entering the premises.

#### 5.1.3 Power and air conditioning

The Data Centre is provided with power backup and is fully air-conditioned.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### **5.1.4 Water exposures**

The Data Centre is protected against water exposures.

#### **5.1.5 Fire prevention and protection**

The Data Centre is protected against fire prevention and protection.

#### **5.1.6 Media storage**

All backup media is stored in a separate location that is physically secure and protected from fire and water damage.

#### **5.1.7 Waste disposal**

No electronic or physical media is disposed of in a manner that access may be gained to it in machine or human readable form.

#### **5.1.8 Off-site backup**

Backups are stored off site at the Disaster Recovery site located at Internet Solutions, Bryanston.

### **5.2 Procedural controls**

The L@Wtrust CA has a number of trusted roles for sensitive operations of the Entrust software used to facilitate the issue of Certificates;

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

To gain access to the software used by the L@Wtrust CA, operational personnel must undergo background investigations. The L@Wtrust CA operations related to adding administrative personnel or changing the CA policy settings require more than one person to perform the operation.

### 5.2.1 Trusted Roles

L@wtrust has identified a number of roles which contribute to the integrity of the L@Wtrust CA and require a high level of trust. A list of these roles is provided below.

#### Entrust Security Manager Roles

- First Officer: Security Officer as defined in the Entrust documentation
- Entrust Master User 1, 2 and 3: start and stop CA services and other sensitive CA activities
- System administrator: Administration of the operation system
- Cryptographic custodian: Person safekeeping cryptographic material.
- Witnesses: Persons performing witness roles of sensitive activities.

#### Encipher Hardware Security Module Roles

- Card holder – Admin 1, 2 and 3: Segregated duties of HSM configuration changes e.g. key generation, key material
- Card holder – Operator 1, 2 and 3: Segregated duties of operational activities.



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 5.2.2 Number of persons required per task;

### Encipher Hardware Security Module Roles

- Admin role: 2 of 3.
- Operator role: 1 of 3.

### Entrust Security Manager Roles;

All roles: either 1 of 1 or one of three.

## 5.2.3 Roles requiring segregation of duties

L@Wtrust enforces a strict segregation of duties with regards to key management activities. The segregation of duties and the trusted role delegation is handled by the L@Wtrust Security Officer and the L@Wtrust Key Manager.

## 5.3 Personnel controls

Operational personnel of the L@Wtrust CA will not be assigned responsibilities that conflict with their responsibilities to the L@Wtrust CA. The operational personnel for the L@Wtrust CA shall be assigned privileges limited to the minimum required to carry out their assigned duties.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 5.4 Audit logging procedures

Significant security events in the L@Wtrust CA are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Authentication codes are used in conjunction with the audit trail files to protect against modification of audit logs. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archive facility.

## 5.5 Records archival

The audit trail files and databases for L@Wtrust CA are both archived. The archive of a L@Wtrust CA's database is retained for at least 3 (three) years. Archives of audit trail files are retained for at least 1 (one) year. The databases for L@Wtrust CA are encrypted and protected by Entrust software master keys. The archive media is protected through storage in a restricted-access facility to which only L@Wtrust CA authorized personnel have access. Archive files are backed up as they are created. Originals are stored on-site and housed with an L@Wtrust CA system. Backup files are stored at a secure and separate geographic location.

## 5.6 Key changeover

Subscribers are issued L@Wtrust Certificates that expire after a defined period of time to minimize the exposure of the associated Key Pair. For this reason, a new Key Pair must be created and that new Public Key must be submitted with each L@Wtrust Certificate Application to replace an expiring L@Wtrust Certificate.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>


## 5.7 Compromise and disaster recovery

L@Wtrust CA's have a disaster recovery plan to provide for timely recovery of services in the event of a system outage.

Entrust requires rigorous security controls to maintain the integrity of the L@Wtrust CA. The Compromise of the Private Key used by an L@Wtrust CA is viewed by Entrust as being very unlikely, however, Entrust has policies and procedures that will be employed in the event of such a Compromise. At a minimum, all Subscribers shall be informed as soon as practicable of such a Compromise and information shall be posted in the L@Wtrust Repository.

## 5.8 L@Wtrust CA or L@Wtrust RA termination

In the event that an L@Wtrust CA ceases operation, all L@Wtrust Certificates issued by such L@Wtrust CA shall be revoked.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 6. TECHNICAL SECURITY CONTROLS

### 6.1 Key pair generation and installation

The signing Key Pair for an L@Wtrust CA is created during the initial start up of the Entrust/Master Control application and is protected by the master key for such L@Wtrust CA. Hardware key generation is used which is compliant to at least FIPS 140-2 level 3.

### 6.2 Private key delivery to subscriber

The applicant shall be responsible for the generation and safeguarding of private keys unless otherwise required in terms of a L@Wtrust RA Charter as approved by the L@Wtrust PA.

### 6.3 Public key delivery to certificate issuer

The Public Key to be included in an L@Wtrust Certificate is delivered to the L@Wtrust CA in a Certificate Signing Request (CSR) as part of the L@Wtrust Certificate Application process.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 6.4 CA public key delivery to relying parties

The L@Wtrust CA public key can be obtained from the L@Wtrust website at <http://www.lawtrust.co.za/repository>.

### 6.4.1 Key sizes

The L@Wtrust CA shall use and issue keys that have a minimum key length of 1024 bits.

### 6.4.2 Key usage purposes (as per X.509 v3 key usage field)

L@Wtrust Certificates issued by the L@Wtrust CA contain the key usage and extend usage Certificates and extensions restricting the purpose for which the L@Wtrust Certificate can be used. Subscribers and relying parties shall only use L@Wtrust Certificates in compliance with this CPS and applicable laws.

## 6.5 Private Key Protection and Cryptographic Module Engineering Controls

The L@Wtrust CA uses Entrust/Authority software in conjunction with hardware certified to FIPPS 140-2 Level 3 to protect the L@Wtrust CA private keys. Subscribers are responsible for protecting the private keys associated with the public key in the L@Wtrust Certificate.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 6.6 Computer security controls

The servers on which the L@Wtrust CA operates are physically secured as described in 5.1 of this CPS. The operating systems on the servers on which L@Wtrust CA operate enforce identification and authentication of users. Access to Entrust Authority software databases and audit trail is restricted as described in this CPS. All operation personnel that are authorised to have access to the L@Wtrust CA are required to use hardware tokens in conjunction with a biometric authentication to gain access to the physical room that contains the Entrust Authority software being used for such L@Wtrust CA.

## 6.7 Life cycle technical controls

The efficacy and appropriateness of the security settings described in this CPS are reviewed on a yearly basis. A risk and threat assessment will be performed to determine if key lengths need to be increased or operational procedures modified from time to time to maintain system security.

## 6.8 Information Security

The L@Wtrust CA shall be subject to generally accepted information security practice.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 7. CERTIFICATE PROFILES

### 7.1 Certificate profile

The profile of a L@Wtrust Certificate will be governed by the profile provided for in the L@Wtrust RA Charter as approved by the L@Wtrust PA.

### 7.2 CRL profile

The profile of a L@Wtrust CRL will be governed by the profile provided for in the L@Wtrust RA Charter as approved by the L@Wtrust PA.

### 7.3 OCSP profile

No stipulation.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The L@Wtrust CA and L@Wtrust RA's shall be audited for compliance against the practices and procedures set forth in this CPS.

### 8.1 Frequency or circumstances of assessment

The L@Wtrust CA and L@Wtrust RA's shall be audited once per calendar year for compliance with the practices and procedures set out in this CPS. If the results of an audit report recommend remedial action, L@Wtrust, the L@Wtrust CA or the applicable L@Wtrust RA shall initiate corrective action within 30 (thirty) days of receipt of such audit report.

### 8.2 Identity/qualifications of assessor

A compliance audit shall be performed by a firm with demonstrated competency in the evaluation of certification authorities and registration authorities.

### 8.3 Assessor's relationship to assessed entity

The entity selected to perform the compliance audit for the L@Wtrust CA and L@Wtrust RA's shall be independent from the entity being audited.



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

#### **8.4 Topics covered by assessment**

The compliance audit shall test compliance of L@Wtrust CA and L@Wtrust RA's set out in this CPS.

#### **8.5 Actions taken as a result of deficiency**

Upon receipt of a compliance audit that identifies any deficiencies, the audited L@Wtrust CA or L@Wtrust RA shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

#### **8.6 Communication of results**

The result of all compliance audits shall be communicated to the L@Wtrust OA and the L@Wtrust PA.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 9. OTHER BUSINESS AND LEGAL MATTERS

### 9.1 Confidentiality of business information

L@Wtrust will not use, disclose or sell applicant or subscriber information, except in accordance with this CPS, Subscriber Agreement or Relying Party Agreement. L@Wtrust, and L@Wtrust RA shall use commercially reasonable care to prevent such information from being used or disclosed for purposes other than those described in this CPS, Subscriber's Agreement or Relying Party Agreement. Notwithstanding the foregoing applicants and subscribers acknowledge that some of the information supplied with a L@Wtrust Certificate Application is incorporated into a L@Wtrust Certificate and that the L@Wtrust CA, L@Wtrust RA and any other parties authorised by L@Wtrust to do so shall be entitled to make such information publicly available.

#### 9.1.1 Scope of confidential information

Information that is supplied by applicants, subscribers or relying parties for the subscription for, use of, or reliance upon a L@Wtrust Certificate, and which is not included in the information described in 9.1.2 below, shall be considered to be confidential. The L@Wtrust CA and L@Wtrust RA's shall be entitled to disclose such information to any sub-contractors or agents that are assisting L@Wtrust in the authentication of the identity of the applicant and the verification of information supplied in L@Wtrust Certificate Applications or that are assisting L@Wtrust in the operation of the L@Wtrust CA or L@Wtrust RA's. Information considered to be confidential shall not be disclosed unless compelled, pursuant to legal, judicial or administrative proceedings, or otherwise required by law. The L@Wtrust CA and L@Wtrust RA's shall be entitled to disclose information that is considered to be confidential to legal and financial advisors assisting in connection with any such legal, judicial, administrative or other proceedings required by law, and to potential

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

acquirers, legal counsel, accountants, bank and financing sources and other advisors in connection with mergers, acquisitions and re-organisations.

### 9.1.2 Information not within the scope of confidential information

Information that is included in a L@Wtrust Certificate or a L@Wtrust Revocation List shall not be considered confidential.

Information contained in this CPS shall not be considered confidential.

Without limiting the foregoing, information that:

- was or becomes known through no fault of L@Wtrust, the L@Wtrust CA or the L@Wtrust RA's;
- was rightfully known or becomes rightfully known to the L@Wtrust CA or a L@Wtrust RA without confidential or proprietary restriction from a source other than the Subscriber;
- is independently developed by L@Wtrust or a L@Wtrust RA; or
- is approved by a Subscriber for disclosure,

shall not be considered confidential.

### 9.1.3 Responsibility to protect confidential information

L@Wtrust, and L@Wtrust RA's shall use commercially reasonable care to prevent such confidential information from being used or disclosed for purposes other than set out in this CPS, Subscriber Agreements or Relying Party Agreements.


	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 9.2 Privacy of personal information

Privacy of personal information shall be protected in terms of the L@Wtrust Privacy Policy published on the L@Wtrust Website at <https://www.lawtrust.co.za/repository>.

## 9.3 Intellectual property rights

L@Wtrust retains all right, title, and interest (including all intellectual property rights), in, to and under all L@Wtrust Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in an L@Wtrust Certificate, which information shall remain the property of the Applicant or Subscriber. All Applicants and Subscribers grant to L@Wtrust and any L@Wtrust RA's operating under the L@Wtrust CA's a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under this CPS, any Subscriber's Agreement, and any Relying Party Agreements. L@Wtrust grants to Subscribers and Relying Parties a non-exclusive, non-transferable license to use, copy, and distribute L@Wtrust Certificates, subject to such L@Wtrust Certificates being used as contemplated under this CPS, Subscriber's Agreement, and any Relying Party Agreements, and further provided that such L@Wtrust Certificates are reproduced fully and accurately and are not published in any publicly available database, repository, or directory without the express written permission of L@Wtrust. Except as expressly set forth herein, no other right is or shall be deemed to be granted, whether by implication, estoppel, inference or otherwise. Subject to availability, L@Wtrust may in its discretion make copies of one or more Cross Certificate(s) available to Subscribers for use solely with the L@Wtrust Certificate issued to such Subscribers. L@Wtrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Cross Certificate(s).

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

L@Wtrust grants permission to reproduce this CPS provided that:

- the copyright notice on the first page of this CPS is retained on any copies of the CPS; and
- this CPS is reproduced fully and accurately. L@Wtrust retains all right, title, and interest (including all intellectual property rights), in, to and under this CPS.

In no event shall L@Wtrust or any independent third-party Registration Authority operating under an L@Wtrust CA, or any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable to any Applicants, Subscribers, or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or any other right of person, entity, or organization in any jurisdiction arising from or relating to any L@Wtrust Certificate or arising from or relating to any services provided in relation to any L@Wtrust Certificate.

#### **9.4 L@Wtrust CA representations and warranties**

L@Wtrust makes the following limited warranties to Subscribers with respect to the operation of L@Wtrust CA's:

- L@Wtrust CA's shall provide Repository services consistent with the practices and procedures set forth in this CPS;
- L@Wtrust CA's shall perform L@Wtrust Certificate issuance consistent with the procedures set forth in this CPS; and
- L@Wtrust CA's shall provide revocation services consistent with the procedures set forth in this CPS.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

Notwithstanding the foregoing, in no event does L@Wtrust, or any L@Wtrust RA or the employees, or directors of L@Wtrust or a L@Wtrust RA make any representations, or provide any warranties, or conditions to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to:

- the techniques used in the generation and storage of the Private Key corresponding to the Public Key in a L@Wtrust Certificate, including, whether such Private Key has been Compromised or was generated using sound cryptographic techniques,
- the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing a L@Wtrust Certificate,
- any software whatsoever, or
- non-repudiation of any L@Wtrust Certificate or any transaction facilitated through the use of a L@Wtrust Certificate, since such determination is a matter of applicable law.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to L@Wtrust Certificates and application using L@Wtrust Certificates are dependent on the transmission of information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of L@Wtrust or a L@Wtrust RA or the employees, or directors of L@Wtrust or a L@Wtrust RA. Neither L@Wtrust nor any L@Wtrust RA or employees, or directors of L@Wtrust or a L@Wtrust RA, shall be liable for any error, failure, delay, interruption, defect, or corruption in relation to a L@Wtrust Certificate, a L@Wtrust Certificate CRL, or a L@Wtrust Certificate Application to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

## 9.5 L@Wtrust RA representations and warranties

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

The same liability provisions that apply in Section 9.4 with respect to L@Wtrust CA's shall apply with respect to L@Wtrust RA's and employees, and directors of the foregoing.

## 9.6 Subscriber representations and warranties

Subscribers and Applicants represent and warrant to L@Wtrust that:

- all information provided by the Subscriber or Applicant to L@Wtrust or to a L@Wtrust RA is correct and does not contain any errors, omissions, or misrepresentations;
- where applicable, the Private Key corresponding to the Public Key submitted by the Applicant or Subscriber in connection with a L@Wtrust Certificate Application was created using sound cryptographic techniques and has not been compromised;
- any information provided to L@Wtrust or to a L@Wtrust RA by the Applicant or Subscriber in connection with a L@Wtrust Certificate Application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;
- the Applicant shall notify the L@Wtrust RA to which it submitted a Certificate Application as soon as practicable if any information included in the Applicant's L@Wtrust Certificate Application changes or if any change in any circumstances would make the information in the Applicant's L@Wtrust Certificate Application misleading or inaccurate;
- the Subscriber shall immediately cease to use the Subscriber's L@Wtrust Certificate if any information included in the Subscriber's L@Wtrust Certificate changes or if any change in any circumstances would make the information in the Subscriber's L@Wtrust Certificate misleading or inaccurate;

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

- the Subscriber shall immediately cease to use the Subscriber's L@Wtrust Certificate upon:
  - expiration, suspension or revocation of the Subscribers L@Wtrust Certificate, or
  - any suspected or actual compromise of the Private Key corresponding to the Public Key in such L@Wtrust Certificate, and shall remove such L@Wtrust Certificate from the devices and/or software in which it has been installed;
- the Subscriber and/or Applicant Shall not use L@Wtrust Certificates for any hazardous or unlawful (including tortious) activities.

## 9.7 Relying party representations and warranties

Relying Parties represent and warrant to L@Wtrust that:

- the Relying Party shall properly validate a L@Wtrust Certificate before making a determination about whether to rely on such L@Wtrust Certificate, including confirmation that the L@Wtrust Certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root;
- the Relying Party shall not rely on a revoked or expired L@Wtrust Certificate;
- the Relying Party shall not rely on a L@Wtrust Certificate that cannot be validated back to a trustworthy root;
- the Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on a L@Wtrust Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by a L@Wtrust Certificate and the importance or value of any transaction that may involve the use of a L@Wtrust Certificate; and



	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

- the Relying Party shall not use a L@Wtrust Certificate for any hazardous or unlawful (including tortious) activities.

## 9.8 Disclaimers of warranties

Except as specifically provided in sections 9.4 and 9.5, neither L@Wtrust, the L@Wtrust CA nor any L@Wtrust RA nor the employees, or directors of any of the foregoing shall make any representations or give any warranties or conditions, whether express, implied, statutory, by usage of trade, or otherwise, and L@Wtrust all L@Wtrust RAs and the employees, and directors of the foregoing specifically disclaim any and all representations, warranties, and conditions of merchantability, non-infringement, title, satisfactory quality, and/or fitness for a particular purpose.

## 9.9 Limitation of liability

Neither L@Wtrust, nor any L@Wtrust RA, nor the employees, or directors of any of the foregoing entities shall be liable for any (a) direct, (b) indirect or special damages and/or (c) loss of income or profit and/or (d) any other form of consequential damages howsoever arising, and regardless of form or cause of action.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 9.10 Force Majeure

Neither L@Wtrust, nor any L@Wtrust RA, nor the employees, or directors of any of the foregoing entities shall be in default hereunder, or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from a failure to perform or comply with the terms of this CPS, any Subscribers Agreement, or any Relying Party Agreement due to any causes beyond its control, which causes include, but are not limited to acts of God or of the public enemy, riots or insurrections, war, accidents, fire, strikes and other labour difficulties, embargoes, judicial action, default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labour, materials, energy, utilities, components for machinery, acts of civil or military authorities.

## 9.11 Individual notices and communications with participants

Unless expressly agreed with any participant to the contrary in writing, or stipulated by the L@Wtrust PA to the contrary, communications addressed to a participant by L@Wtrust, the L@Wtrust CA or a L@Wtrust RA may, at the foregoings discretion, be communicated by email to the email address provided by the participant.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 9.12 Amendments

### Procedure for amendment:

- L@Wtrust PA shall consider the provisions of this CPS, any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or L@Wtrust RA Charter, previously approved by at least annually and shall also consider proposals for amendment that may be received from the L@Wtrust OA or a L@Wtrust RA.
- A proposal for an amendment to this CPS or to any documents, including without limitation, a Subscribers Agreement, Relying Party Agreement, or L@Wtrust RA Charter, previously approved by the L@Wtrust PA shall be submitted to the L@Wtrust PA for consideration.
- The L@Wtrust PA shall within a period of not more than 60 (sixty) days from the date of receipt of the proposal, consider the proposal and determine whether the proposal for amendment well founded and an amendment warranted.
- Once an amendment has been drafted it shall be considered by the L@Wtrust PA taking into account good practice relating to the PKI, information security and the needs and best interests of the participants to the PKI.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

### **Notification mechanism and period**

- The L@Wtrust PA shall determine the notification mechanisms and period before which an amendment may become effective in each instance and provide written directives in this regard.
- The L@Wtrust PA shall exercise reasonable care to ensure that the mechanism of notification and the period of notification do not prejudice participants in the PKI and are in the best interests of the proper and secure operation of the PKI

### **9.13 Dispute Resolution**

If the matter in dispute is primarily a legal matter then the Arbitrator shall be an advocate practising at the Johannesburg Bar and shall be appointed by agreement between the parties. If the parties are unable to agree as to the appointment of an Arbitrator within 7 (seven) days of the arbitration being demanded by any party, then he shall be appointed by the Chairman at the time of the Johannesburg Bar Council within 7 (seven) days of being requested to do so by any party. Should the Arbitrator deem it necessary to obtain technical advice on any matter relating to the dispute he shall be entitled to obtain such advice from a technical expert in the relevant field.

If the matter in dispute is primarily a technical matter then the Arbitrator shall be an expert in the matter under dispute appointed by agreement between the parties. If the parties are unable to agree as to the appointment of an Arbitrator within 7 (seven) days of the arbitration being demanded by any party, then he shall be appointed by the Chairman at the time of the Computer Society of South Africa within 7 (seven) days of being requested to do so by any party.

	<b>Classification</b>	<b>LEVEL 1 Public information</b>
	<b>Reference</b>	<b>LT_ISP_IS_CP_01.doc</b>
	<b>Location</b>	<b><a href="http://www.lawtrust.co.za/repository">http://www.lawtrust.co.za/repository</a></b>
	<b>Version</b>	<b>13-02-2007</b>
	<b>Policy Authority</b>	<b>L@Wtrust PA</b>

## 9.14 Governing Law

The entire provisions of this CPS and any Subscriber's Agreement or Relying Party Agreement entered into pursuant to this CPS shall be governed by and construed in accordance with the laws of the Republic of South Africa. Furthermore, the parties hereto irrevocably and unconditionally consent to the non-exclusive jurisdiction of the Johannesburg Magistrate's Court or the Witwatersrand Local Division of the High Court of South Africa, as the case may be, in regard to the enforcement of any rights relating to all matters arising from this CPS.

## 9.15 Miscellaneous Provisions

### 9.15.1 Entire Agreement

The provisions of this CPS and/or Subscribers or Relying Party Agreements, as the case may be, constitute the entire contract between the applicable parties with regard to matters dealt with in this CPS and those agreements. No representations (save for any fraudulent misrepresentations) terms, conditions or warranties not contained in this CPS and/or Subscriber or Relying Party Agreements, as the case may be, shall be binding on the parties.

### 9.15.2 Severability

To the extent that any provisions of this CPS or Subscriber or Relying Party Agreements, as the case may be, may be struck-out as unlawful, only those provisions shall be severed from this CPS or a Subscriber or Relying Party Agreements and all other provisions of this CPS or Subscriber or Relying Party Agreements shall remain of full force and effect, notwithstanding the severing of those provisions.