L@Wtrust information security solutions	INFORMATION SECURITY POLICY
	ISSUE SPECIFIC POLICY
	VERSION: 13-02-2007
	EFFECTIVE DATE: 01-03-2007

Certificate Policy

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 • Email governance@lawtrust.co.za

L@Wtrust reserves the right to change or amend this certificate policy 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.

Table of Contents

Note: *please refer to the definitions set out in Appendix D (page 16) when considering the information contained in this certificate policy.*

1 Purpose

Law Trusted Third Party Services (Pty) Ltd ("L@Wtrust") [*www.lawtrust.co.za*] conducts the business of providing trusted third party authentication and public key cryptography services. These services include (i) appointing third party customer Registration Authorities ("RA"), (ii) training and monitoring certificate administrators appointed by RA's, (iii) the issuing of digital certificates by the certificate authority it operates ("L@Wtrust CA"), (iv) managing the lifecycle of digital certificates issued, (v) providing reference information on the status of all digital certificates issued.

Digital certificates, containing a public key, identify the person who is the holder of the associated private key used to digitally sign an electronic transaction. This forms the basis of positive identity, message integrity, and non-repudiation when conducting business electronically. Private keys may also be used to achieve confidentiality.

This L@Wtrust Certificate Policy introduces the rules that L@Wtrust requires adherence to in order to ensure a high level of trust in the digital certificates issued by the L@Wtrust CA. Digital certificates, properly issued, are an effective risk management tool used address the business need for positive identity, privacy and non-repudiation.

2 Scope

The management of the resources required to operate the L@Wtrust CA is in accordance with the provisions contained in the L@Wtrust certification practice statement ("L@Wtrust CPS"). These resources include registration authorities, personnel, network infrastructure, IT systems, cryptographic material, physical locales, and information assets.

3 Policy Statements

3.1 L@Wtrust CPS

All digital certificates are issued in accordance with the L@Wtrust certification practice statement ("L@Wtrust CPS"). The L@Wtrust CPS defines the practices and procedures that L@Wtrust and/or customer RAs employ in identification, authentication, issuing, managing, revoking, and renewing digital certificates. The L@Wtrust CPS is based on the L@Wtrust certificate policy, the practices and policies of Entrust, Inc. [*www.entrust.com*], the Electronic Communication and Transactions Act, 2002, international public key infrastructure standards (e.g. PKCS for X509 v.3 format certificates), L@Wtrust's information security policies (i.e. enterprise, system specific, and issue specific policies), L@Wtrust's shareholder requirements, and most importantly L@Wtrust's customer requirements.

3.2 Digital certificate intended usage

Digital certificates issued by the L@Wtrust CA are intended for the following purposes: (i) prove identity to a remote information system, (ii) protecting email messages, (iii) Online Certificate Status Protocol (OCSP) response signing, (iv) Entrust Event certificate signing, (v) PKIX-CMP signing, (vi) smart card Logon, (vii) Encryption and Signing purposes. All digital certificates issued by L@Wtrust may only be used for lawful purposes.

3.3 Subscriber identification and authentication

A subscriber is required to: (i) complete and sign a personal digital certificate application form and a subscriber's agreement; (ii) present his/her identity document, passport or drivers licence, to a certificate administrator. After authenticating the identity of the subscriber, the information contained in the personal digital certificate application form, and the signatures of the subscriber on the personal digital certificate application form and the Subscriber's Agreement, the L@Wtrust CA will issue a digital certificate to the subscriber.

3.4 Publication of a digital certificate status

The status of a digital certificate issued by the L@Wtrust CA, i.e. information on whether a digital certificate has been revoked and at what time, appears in the L@Wtrust certificate revocation list, as updated from time to time, the most recent copy of which is published at *http://crl.lawtrust.co.za*.

3.5 Subscriber private key protection

A Subscriber is required to protect the private key associated to the digital certificate issued by the L@Wtrust CA by maintaining the confidentiality thereof. This may include: (i) using adequate password controls, (ii) up to date antivirus/spyware protection mechanisms, (iii) data back ups, (iv) cryptographic tokens to store the private key.

3.6 Issuer private key protection

L@Wtrust appreciates the importance of guarding against the risk of compromise of a CA's private key(s) and, as such, implements appropriate controls to ensure the continued security of its private key(s). An outline of these measures is published in the L@Wtrust CPS. Such mechanisms include: (i) the private key material must be stored inside a hardware security module, (ii) all cryptographic operations will be performed inside of a hardware security module, (iii) access to sensitive operations on the hardware security module is restricted and controlled via segregation of duties, (iv) all personal participating in sensitive cryptographic functions will have undergone reasonable clearance procedures in order to establish a high level of trust.

3.7 X509 V3 Mandatory Field requirements

The following digital certificate fields are set out in annexure C attached hereto: Version Number, Serial Number, Signature Algorithm, Issuer, Validity Dates, Subject, Public Key Algorithm, Public Key Minimum Length, and other appropriate fields, for example any Required Extensions.

4 Obligations and Liabilities

4.1 Subscriber

All obligations and liabilities of a subscriber, i.e. the person applying to be issued with a digital certificate, are governed by the terms and conditions contained in the L@Wtrust subscriber agreement, which includes: (i) providing and guaranteeing the accuracy of information in a certificate application and the acceptance of a certificate, (ii) protecting the access to the private key associated to the certificate issued, (iii) notification of private key compromise or change of status, (iv) restrictions of the use of the certificate to the usage specified, and (v) ensuring relying parties are made aware of the provisions of any applicable relying party agreement. The most recent copy of the subscriber agreement is available for download from the L@Wtrust website. You may consider the version of the subscriber agreement available for download from the L@Wtrust website (www.lawtrust.co.za/repository) as the most current version as at the time of downloading.

4.2 Issuer

All obligations and liabilities of the Issuer, i.e. the L@Wtrust CA and/or LAWtrust RA(s) including the certificate administrator(s), are governed by provisions contained in the L@Wtrust CPS, which include: (i) notification that a certificate has been revoked, (ii) making available certificate status to relying parties (certificate revocation list), (iii) being audited for compliance against stipulated practices and procedures, (iv) disclaimers and limitation of liability, and (v) confidentiality protection to non-public subscriber and relying party information. The most recent copy of the L@Wtrust CPS is available for download from the L@Wtrust website. You may consider the version of the L@Wtrust CPS available

for download from the L@Wtrust website [*www.lawtrust.co.za/repository*] as the most current version as at the time of downloading.

4.3 Relying Party

All obligations and liabilities of a relying party, i.e. a person (recipient) who has received a digitally signed data message and is relying on the contents of a digital certificate and the digital signature to (i) identify the person who signed that message, and (ii) confirm the correctness (integrity) of the contents of the message itself, are governed by the terms and conditions contained in the L@Wtrust relying party agreement, which includes: (i) applicable usage, (ii) liability exclusions, limitations and warranties, and (iii) validating the digital signature and its associated digital certificate.

5 Security Management

L@Wtrust manages its information security through an information security management program ("ISMP"). Two Authoritative bodies comprising of senior management have been established to manage the L@Wtrust ISMP. The L@Wtrust Policy Authority ("L@Wtrust PA") is 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.

5.1 Policy Structure

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, RA Charter etc…)

5.2 Policy Administration

A L@Wtrust Policy Authority ("L@Wtrust PA") is set up to manage the lifecycle of the Certificate Policy. The L@Wtrust Operating Authority ("LAWTrust OA") is setup to ensure that the practices and controls specified in the cps fully support the CP. The L@Wtrust PA may, from time to time, amend the provisions of this CP. You may consider the version of the CP available for download from the L@Wtrust website (www.lawtrust.co.za/repository) as the most current version as at the time of downloading. The L@Wtrust PA may be contacted on governance@lawtrust.co.za.

6 Governing Law

The laws of the Republic of South Africa, as amended.

7 Related documentation

	Reference	Name	Exposure
1	LT_ ISP_01.doc	L@Wtrust Information Security Policy	Level 2: Internal
2	LTP_ISP_IS_CPS_01.doc	L@Wtrust Certificate Practice Statement	Level 1: Public

Appendix A [Approval]

PRIMARY

APPROVAL		
Name and Title:	LT_CP_01.doc – L@Wtrust Certificate Policy	
Version:	1.00	
Effective Date:	01/03/2007	
Approved by ISF:	*Signature of Chairman of ISF*	*Date Approved*

SECONDARY

ADDITIONAL APPROVAL REQUIRED BY ISF		
NAME / ROLE	**SIGNATURE**	**DATE**

Appendix B [Revision History]

Version/Revision No:		
Date of Revision:		
Revision Purpose:		
Version/Revision No:		
Effective Date:		
Approved by ISF:	*Signature of Chairman of ISF*	*Date Approved*

Appendix C [Digital Certificate Specification]

L@Wtrust Certificate Profile Summary Table (part 1)

Field Type	Field Name	Value	Example	Explanation
X509 Version 1 fields	Version	V3	V3	As specified in X509 Version 3.
	Serial Number	a unique integer represented in Hexadecimal	44 F2 DE E2	Each certificates issued by the L@Wtrust CA is allocated a unique number.
	Signature Algorithm	SHA1/RSA		Algorithm to produce signatures
	Issuer	DN	CN = LAWtrust CA O = LAWtrust C = ZA	Entries describing the Issuer in terms of the DN.
	Valid from	Date, Time	Not valid before: date (03 October 2006 08:36:52 AM)	
	Valid to	Date, Time	Not valid after: date (03 October 2007 09:06:52 AM)	
	Subject	DN	E = name@lawactive.co.za CN =Firstname Surname Serial Number = LAWtrust O = LAWtrust Personal O = LAWtrust C = ZA	Subject details of the certificate. This uniquely identifies the subscriber. This is a variable set of fields and values.
	Public Key	RSA 1024 bit keypair	30 81 89 02 81 81 00 d1 e7 b0 7f bb f6 2e 8f 56 e7 13 1a 00 63 d8 6f 39 ba bd 7e c7 e5 44 c0 47 bb 1b 00 a8 7a 33 a3 69 7f 1a af 15 3b fa 5b fe b1 b0 e5 86 68 fc 17 99 b8 8c 44 c9 64 79 dd 2c c5 5b 3b 43 a4 a8 b9 99 46 50 f5 21 9d 22 d2 26 38 72 29 f3 66 be 1e fa 46 0d 40 1c 6c 26 44 7e c1 69 19 1c c7 47 82 71 66 45 a5 42 0d 6c be 03 e2 7f 78 d6 2a b3 dd 9e d9 6d 9a 84 63 ee 0f 1e 4c 33 36 4b e2 56 13 02 03 01 00 01	The public Key unique to each subscriber

L@Wtrust Certificate Profile Summary Table (part 2)

Field Type	Field Name	Value	Example	Explanation
Certificate Extensions	Key Usage	Digital Signature Key Encipherment	Digital Signature and Key Encipherment	Specifies practical usage of certificate
	Private key usage period	Not valid before: date Not valid after: date	Not before=03 October 2006 06:36:52 AM Not after=03 October 2007 07:06:52 AM	Dates within which the private key is valid.

	Netscape Cert Type	cert type	SSL Client Authentication, SMIME	Netscape usage
	Certificate Policies	URL	[1]Certificate Policy: Policy Identifier=Certificate Policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.lawtrust.co.za/repository	The L@Wtrust documentation governing the CA and certificate usage is published at https://www.lawtrust.co.za/repository. The documentation set includes Policies, Practices and Agreements
	CRL Distribution Points	URL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.lawtrust.co.za/lawtrust.crl [2]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=LAWtrust CA O=LAWtrust C=ZA	The L@Wtrust CA will issue CRLs and make them available via 1] http at http://crl.lawtrust.co.za. 2] ldap directory. ldap://196.38.133.226:389/cn=CRL1,cn=LAWtrust CA,o=LAWtrust,c=ZA The CA will issue at least one crl publication by the end of each business day.
	Authority Key Identifier		KeyID=01 2f a9 9f d3 11 2b bb ff 9e 9a 11 87 06 40 6d 08 b4 79 3f	The Authority Key Identifier is used by path validation software to help identify the next certificate up in a certificate chain. This extension can contain a keyIdentifier which is typically a hash based on the authority certificate's public key and/or fields containing the authority certificate's Subject Name and Serial Number.

L@Wtrust Certificate Profile Summary Table (part 3)

Field Type	Field Name	Value	Example	Explanation
Certificate Extensions (continued)	Subject Key Identifier		9f 85 15 2a 44 81 67 5b 33 90 30 d9 aa 26 cc 24 80 0e a8 37	The Subject Key Identifier is used by path validation software by helping to identify certificates that contain a particular public key.
	Basic Constraints		Subject Type=End Entity Path Length Constraint=None	Constraints description
	Entrust Version Info		Entrust Authority Security Manager Version=V7.1 Key Update Allowed=Yes Certificate Category=Web	Information specifying the Version of the Entrust Security Manager Software

Certification Hierarchy	Certification Path		Entrust.net Secure erver Certification Authority ↳LAWtrust CA ↳User Name	An ordered sequence of certificates of entities which, together with the public key of an initial enity in the path, can be processed to obtain the public key of the final entity in the path

Appendix D [Definitions]

asymmetric cryptosystem	See definition of cryptography
authenticate/ authentication	Authentication: verification of an individuals claimed identity: a) at registration, the act of evaluating the subscribers' credentials as evidence for their claimed identity; b) during use, the act of comparing electronically submitted identity and credentials (i.e. user ID and password) with stored values to prove identity.
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.
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.
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: 1. decrypting the signature object with the public key component to expose the original hash value, 2. re-computing a hash value over the data object, and 3. comparing the exposed hash value to the re-computed hash value. If the two values are equal the signature is often considered valid.

digitally sign	The act of generating a digital signature for a data message, which is created by: 1. Hashing the object to be signed with a one-way hash function; and 2. Encrypting (signing) the hash value with the private key component of a key pair. The hash value is encrypted instead of the data itself because the encryption function is typically very slow compared to the time it takes to complete the hash of the data. The object created by these two steps is called the signature and is bound to the data message according to an application specific mechanism.
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.
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.
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.
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.