LDRC CERTIFICATE POLICY FOR THE MANITOBA LEGAL PROFESSION

The Certificate Policy of
Legal Data Resources (Manitoba) Corporation (LDRC)
and The Law Society of Manitoba (LSOM)
for X.509 Digital Certificates for the Manitoba Legal Profession
and relying Government or Courts Parties

Release Version 1.01: December 1, 2012

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

In order to improve the quality of service within and provided by the Manitoba legal profession, LDRC and LSOM have implemented a public key infrastructure (PKI) that enables participating members of the profession, relying parties and others to securely and privately exchange electronic data over the Internet through the use of public key cryptography. A public key is an extremely long binary string stored in a computer file which users (subscribers) principally generate themselves, using supplied software. A subscriber's public key can then be made available to other users participating in the system for the purpose of encrypting e-mail messages addressed to the subscriber, and once a message is so encrypted, the subscriber alone has the capability to decrypt the message. In the process of generating keys, the subscriber also generates a private key, held only by such subscriber, which is used for the decryption of the messages which have been encrypted using that subscriber's public key. Public keys can also be used in conjunction with a subscriber's private key so as to create a digital signature and thereby to conclusively identify users delivering messages. The supplied software for generating a public/private key pair under this PKI and this Certificate Policy, and the key pair itself, both adhere to international standards established by the Internet Society and the Internet Engineering Task Force (IETF). Under this PKI, LDRC will issue X.509 digital certificates to subscribers authorized by LSOM.

The role of the "digital certificate" is to associate a person's public key with that person, and, in this implementation, to identify a subscriber as a lawyer entitled to practice law in the Province of Manitoba. A subscriber's digital certificate will include, among other things:

(1) a serial number that uniquely identifies the certificate;

(2) the common name that identifies the subscriber;

(3) the unique public key value associated with the common name;

(4) information identifying LDRC as the certificate issuer;

(5) LDRC's digital signature; and

(6) the unique number (Object Identifier or OID) identifying this PKI implementation and this Certificate Policy.

The subscriber, uses supplied software to create, or in limited instances has created for such subscriber, a private key that is uniquely associated with the subscriber's public key included in the certificate. When a subscriber uses his or her private key to send, encrypt or sign an electronic message or document, the subscriber's certificate is attached to the message or document and, assuming the integrity of the system based on subscriber protection of private keys, the subscriber cannot repudiate the fact that it was sent or signed by him or her because

such signature uses a process uniquely available to that subscriber. By using the recipient's public key to encrypt a message, the subscriber can also be assured that the message can only be read by its intended recipient, so long as the integrity of the system based on subscriber protection of private keys is maintained. The recipient (the "relying party") can also use the certificate system to verify that it was sent or signed by the person identified in the certificate.

This PKI implementation is intended to implement a non-repudiation digital certificate environment for lawyers in Manitoba, in order to assure governmental and other authorities of the legitimacy and authenticity of digital signatures used for such filing systems and in order to induce governmental and other authorities to proceed with systems requiring secure transmission of intended-recipient-only messages.

1.1.1 Certificate Policy Purpose Overview

This Certificate Policy is a statement of the policies established by LDRC and approved by LSOM for the issuance, control, use and management of the digital certificates issued or to be issued under this Certificate Policy to members of the Manitoba legal profession and others. It is adapted from the certificate policy framework published by the Internet Engineering Task Force (IETF) as RFC 3647. Any questions about it should be directed to LDRC.

This Certificate Policy is supported by a Certification Practice Statement that establishes the practices employed by LDRC in issuing, managing, renewing and revoking digital certificates. It is also supplemented by a PKI Subscription Form that provides initial overview information about this Certificate Policy. Together, these documents form part of the LDRC/LSOM public key infrastructure.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is called the LDRC Certificate Policy December 1-2012v4.docRelease Version 1.01"

Various agencies have defined a trust framework that sets out common requirements for electronic credentials in 4 different assurance levels. An assurance level describes the degree to which a Relying Party in an electronic business or other transaction can be confident that the credential being presented actually represents the person or entity named in it and that it is the represented person or entity who is actually engaging in the electronic transaction. The 4 levels are identified by both a number and a text label and are based on NIST *Special Publication 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, as follows:

Table 1-1: Electronic Credential Assurance Levels

Number	Label	Description
1	Minimal	Little or no confidence in the asserted identity's validity
2	Moderate	Some confidence in the asserted identity's validity
3	Substantial	High confidence in the asserted identity's validity
4	High	Very high confidence in the asserted identity's validity

This CP defines policies for the issuance of digital certificates under the above 4 assurance levels. Unless explicitly stated otherwise, all stipulations of this CP are applicable to certificates issued under all of the above 4 assurance levels. Assurance levels may be stipulated by relying parties for transactions from time to time but in the absence of a specific stipulation, level 4 assurance should be assumed by subscribers to be associated with use of certificates under this policy.

This Certificate Policy is expected to be assigned a number as its unique Object Identifier (OID) by the Canadian International Standards Organization Registration Authority (COSIRA) or its delegated or successor organization . This OID forms part of each certificate issued under this Certificate Policy and allows a relying party to consult this document when reviewing electronic data accompanied by a digital certificate issued under this Certificate Policy.

This Certificate Policy may be cited as the "LDRC Certificate Policy for the Manitoba Legal Profession".

1.3 PKI PARTICIPANTS

The following table illustrates the relationships of the Digital ID CA individuals to PKI and Entrust roles:

Table 1-2 PKI and Entrust Roles

Individual	PKI Role	Entrust Role
Executive Management **Members of the Manitoba LDRC Board of Directors** **Executive Management of LSOM**	PKI Policy Setting; Oversight	N/A
Cryptographic Custodians The Cryptographic Custodians (CC) are responsible for providing multi-person control over the secure storage of CA security sensitive items (LDRC System Administrator, LDRC Administrator, LSOM IT Administrator).	PKI Security Officer Administrator (SA) PKI Initiation	Entrust SA Entrust Initiation/Control
Master Users The Master Users (MU1/2/3) will be required to start and stop CA services (LSOM Manager LDRC Chair, LSOM Systems Administrator).		
System Administrator LDRC System Administrator (SA)	PKI Operations Administrator	Entrust Administrator
PKI Security Officer PKI Security Officer (SO) LDRC System Administrator.	First Officer	Entrust SA
OA System Administrator (system) LDRC Administrator	System Administration (Operating System)	N/A
Senior Production Control Analyst	Entrust CA Administrator	Security Officer
Production Control Analyst	First Officer	Entrust Administrator

Individual	PKI Role	Entrust Role
Compliance Analyst	Auditor	Entrust Auditor
Help Desk or Customer Service Representative or Client	First Officer	Entrust Administrator
Employee or Customer **Relying Party**	Subscriber, Certificate Holder	Certificate Subject

1.3.1 Certification Authority

The LDRC CERTIFICATION AUTHORITY (CA) has been created using Entrust Limited's root certificate and LDRC is responsible for this CA instance. For this purpose, LDRC holds a self-signed root certificate and is responsible for independently issuing certificates to subscribers and revoking certificates issued by it. It is also responsible for administering this Certificate Policy and maintaining the infrastructure required for the LDRC/LSOM PKI. LDRC may carry out its responsibilities under this Certificate Policy through its employees or, when expressly authorized by its Board, through external agents or representatives. If responsibilities are delegated, LDRC remains responsible for ensuring compliance with this Certificate Policy. LDRC is also entitled to apply to the LSOM where it believes professional practice standards have not been met with the use of public and private keys issued to a member under this Policy.

1.3.2 Registration Authority

LSOM is the Registration Authority. As such, it identifies eligible subscribers and their entitlement to hold certificates through a database which has been made available to LDRC (hereinafter referred to as the PKI database). It also provides notice of the revocation of such eligibility through that same database and by that process initiates the revocation of a certificate. (See section 3.5)

1.3.3 End Users

End users consist of subscribers and other relying parties.

Subscribers are primarily lawyers who are entitled to practise law in Manitoba, but may include others who require certificates for electronic communications with lawyers or others under a program for whom the use of certificates has been approved under this Certificate Policy by LSOM.

A relying party is any person or entity that:

(1) receives an electronic message or document that is associated with a certificate; and

(2) relies on the certificate to verify the identity of the sender or signer of the message or document.

1.3.4 Subscribers

Subscribers are members of the legal profession in the Province of Manitoba (or members of the legal profession in other provinces of Canada authorized to participate in the PKI by the LDRC Board of Directors and LSOM).

1.3.5 Relying Parties

Relying parties are members of government departments of the Government of Canada, the Province of Manitoba, the City of Winnipeg or other members or elements of governments, municipalities or outside parties authorized to use LDRC Certificates by the LDRC Board of Directors and LSOM that use a certificate issued under this Certificate Policy and signed by the CA to authenticate a digital signature or encrypt communications to a certificate holder or an authorized outside party based upon an arrangement between the department or other party and LDRC for such use as described in 1.4 below. Other use may be announced by LDRC as identifying authorized recipient parties by a posting on the LDRC web site (www.LDRC.org). Departments of governments or municipalities or individuals or outside entities other than those so announced and authorized are not entitled to rely on certificates issued by the CA and, any such reliance is done at their own risk. Further where a subscriber makes use of a certificate for an unauthorized use, LDRC may immediately revoke that subscriber's certificate in LDRC's sole discretion.

1.4 CERTIFICATE USAGE

A digital certificate is to be used only for the following purposes:

(1) by the subscriber to send digitally signed electronic messages or documents;

(2) to another subscriber;

(3) to a court in Manitoba (in accordance with the applicable policies of the court);

(4) to any department, branch or agency of the Manitoba or Canadian government or the City of Winnipeg that has endorsed the use of certificates for that purpose;

(5) by the subscriber to encrypt electronic messages or documents for delivery to another subscriber or for the secure storage of the information;

(6) by a relying party to identify and authenticate the subscriber when he or she sends or signs an electronic message or document using his or her private key; and

(7) in the case of electronic transactions for which the use of certificates is approved under this Certificate Policy, by the subscriber to participate in the transaction, and by a relying party to identify the subscriber and communicate with the subscriber.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This Certificate Policy is to be administered by LDRC in accordance with a confirmation letter from LSOM to LDRC. Unless otherwise directed by LDRC, all questions about this policy are to be directed to the contact for LDRC (see s. 1.5.2).

1.5.2 Contact Person

For LDRC:

Executive Director
Legal Data Resources (Manitoba) Corporation
102 – 400 St. Mary Avenue
Winnipeg, Manitoba, Canada R3C 4K5
e-mail: admin@ldrc.net
phone: (204) 984-9840
fax: (204) 949-0770

For LSOM:

Chief Executive Officer
The Law Society of Manitoba
219 Kennedy Street
Winnipeg, Manitoba, Canada R3C 1S8
e-mail: lawsociety.mb.ca
phone: (204) 942-5571
fax: (204) 956-0624

1.5.3 Publication of Certificate Policy

This Certificate Policy, as amended from time to time, is to be published on the LDRC website.

1.5.4 Amendment process

This Certificate Policy may be amended by LDRC, but only with the approval of LSOM.

No amendment will take effect until it receives the approval of the President of LDRC and the CEO of LSOM, any required registration is completed and it is published on the LDRC website.

1.5.5 Person Determining CPS Suitability for the Policy

The CPS is administered by the LDRC Administrator and Network Administrator as OA and is approved by the PMA. Suitability is determined by the PA prior to presentation to the PMA and RA for approval.

1.5.6 CPS Approval Procedures

The PMA approves this CPS and any subsequent changes prior to promulgation. Changes are drafted by the OA and reviewed by the PA, for CP compliance, prior to presentation to the PMA.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

The following definitions and acronyms apply in this Certificate Policy:

Certificate Authority or **CA** — the entity responsible for issuing, managing and revoking certificates (which is LDRC under this Certificate Policy).

Certification Practice Statement — the statement describing the standards, procedures and practices that are established by LDRC and approved by LSOM for the implementation of this Certificate Policy.

digital certificate — a root certificate (defined in this section) or a subscriber's digital certificate (described in section 1.1).

end user — a subscriber or other relying party.

asymmetric key — a long binary string that is uniquely associated with a subscriber and is used by a software application to perform a function. Keys are generated by software or cryptographic hardware in pairs consisting of a **private key** and a **public key** that are uniquely associated with each other. A **private key** is used by a subscriber to associate his or her digital certificate with an electronic message or document, thereby allowing it to be identified as his or her message or document. A **private key** is also used to decrypt a document that was encrypted for a subscriber with his or her **public key**.

LDRC — Legal Data Resources (Manitoba) Corporation.

LSOM — The Law Society of Manitoba.

Object Identifier or **OID** — a unique character string assigned to an object such as this Certificate Policy to signify registration with Internet registering entities such as COSIRA.

PA — means the President of LDRC and a director chosen by resolution of the LDRC from time to time as as second member fo the policy authority for this PKI.

PKI — a public key infrastructure (described in section 1.1). **LDRC/LSOM PKI** refers to the public key infrastructure governed by this Certificate Policy. **LSOM PKI database** refers to the private database or databases created by LSOM and used by LDRC to authenticate eligible subscribers.

Policy Management Authority — the policy management authority is the Board of Directors of LDRC and the CEO of LSOM.

Registration Authority or **RA** — the entity responsible for authenticating eligible subscribers for digital certificates (which, under this Certificate Policy, is LSOM).

relying party — a person or government office holder who relies on the digital certificate associated with an electronic message or document to identity the person who sent or signed the message or document.

repository — the repository of information to be maintained by LDRC under this Certificate Policy for the benefit of participants in the LDRC/LSOM PKI.

root certificate — the digital certificate issued by a widely trusted Certificate Authority (in this case Entrust Limited) to LDRC, which permits a further digital certificate to be generated by LDRC for the purpose of enabling the LDRC PKI (the LDRC root certificate). The root certificate forms the start of the chain of trust that a relying party relies upon to verify the identity of the subscriber identified by the subscriber's digital certificate. In this chain of trust, a subscriber's digital certificate is subordinate to the root certificate.

subscriber — means parties qualified as such under section 1.3.3 of this Certificate Policy and depending on the context, is either:

(a) a person in whose name a digital certificate is issued under this Certificate Policy; or

(b) an applicant for a digital certificate to be issued by under this Certificate Policy.

1.6.2 Acronyms

The standard list of acronyms for this CPS (including amendments) follows:

ARL	Authority Revocation List
CA	CERTIFICATION AUTHORITY
CAST	Symmetric Cipher named after the inventors **C**arlisle **A**dams and **S**tafford **T**avares
CCTV	Closed circuit television
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAP	Directory Access Protocol
DES	Data Encryption Standard

DN	Distinguished Name
DNS	Domain Name Server
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
FIPS	Federal Information Processing Standard
HR	Human Resources
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
RA	Registration Authority
OA	Operational Authority
OID	Object Identifier
PA	Policy Authority
PMA	Policy Management Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PUB	Publication
RDN	Relative Distinguished Name
RFC	Request For Comments (IETF)
RSA	Rivest-Shimar-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SEP	Secure Exchange Protocol
SHA-1	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The CA shall operate at least one Repository in which encryption certificates issued to End Users as well as CRLs and ARLs are stored. The CA shall ensure unrestricted End User access to CRLs and ARLs.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

For the use of its Subscribers and Relying Parties, the CA shall publish the following information to a Repository (directory, databases, web server, etc.):

- Issued certificates;
- CRLs/ARLs;
- The CA's certificate associated with its signing key;
- This CP; and
- Any relevant information that is necessary for reliance on certificates issued under this CP.

The CA shall not publish the CPS.

2.3 TIME OR FREQUENCY OF PUBLICATION

All information to be published in the Repository shall be published as soon as such information is available to the CA. Certificates shall be published immediately following user acceptance as specified in section 5.4.1 and proof of possession of a private key as specified in section 5.1.5. Information regarding frequency of CRL/ARL publication is found in section 5.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

The CA shall protect any Repository information not intended for public dissemination or modification and no access to the Repository or the information, except as expressly authorized under this Certificate Policy will be permitted. Public Key certificates and certificate status information in the Repository shall be publicly available to participants in this PKI through the CA. Where applicable, access privileges to information stored or controlled by the CA shall be determined initially by the OA and approved by the PA.

3. GENERAL RESPONSIBILITIES OF SERVICE PROVIDERS AND END USERS

3.1 General Responsibilities of Trust Service Providers

The general responsibilities of a trust service provider (LDRC, LSOM and any entity to whom any of their responsibilities is delegated) are in addition to any other specific responsibility of the trust service provider under this Certificate Policy.

3.1.1 LDRC's general responsibilities as Certificate Authority

LDRC, as the Certificate Authority under this Certificate Policy, is responsible for:

(1) administering this Certificate Policy in accordance with its terms and the specific delegation arrangements between LDRC and LSOM;

(2) ensuring that digital certificates are issued, managed and revoked in accordance with this Certificate Policy;

(3) maintaining and providing access to a reasonable availability information repository;

(4) observing the rights of subscribers and relying parties who use certificates in accordance with this Certificate Policy and all applicable laws and agreements;

(5) providing online and support phone guidance for persons participating in the LDRC/LSOM PKI;

(6) publishing this Certificate Policy in a manner that makes it accessible to all persons participating in the LDRC/LSOM PKI;

(7) notifying subscribers of any changes to this Certificate Policy;

(8) keeping confidential — and maintaining strict control procedures for the security of — any private keys held by it, as well as any passwords, passphrases, PINs or other secrets used in obtaining access to PKI facilities;

(9) using LDRC's private key created for the purpose of managing certificates only for that purpose, including for signing certificates and certificate status information;

(10) issuing and revoking certificates based on the LSOM PKI database;

(11) revoking a certificate at the authenticated request of the subscriber;

(12) supplying public certificate information to the repository promptly after it is issued;

(13) supplying certificate status information to the repository;

(14) maintaining a current certificate revocation list and supplying regular updates to the repository;

(15) protecting information in the repository from unauthorized modification; and

(16) conducting periodic reviews of this Certificate Policy and amending it from time to time with the approval of LSOM.

LDRC may, with the approval of LSOM, delegate any of its responsibilities under this Certificate Policy, but remains responsible for ensuring that the delegated responsibilities are carried out in accordance with this Certificate Policy.

3.1.2 LSOM's general responsibilities as Registration Authority

LSOM, as the Registration Authority under this Certificate Policy, is responsible for:

(1) authenticating eligible subscribers in accordance with this Certificate Policy and the agreement between LSOM and LDRC;

(2) updating the LSOM PKI database to initiate a revocation request if a subscriber is no longer eligible for a certificate;

(3) promptly notifying LDRC if it receives notice that a subscriber's private key has become compromised;

(4) providing supplementary information to LDRC when required for LDRC to issue a certificate to a subscriber or to revoke a subscriber's certificate; and

(5) keeping confidential — and maintaining proper control procedures for the security of — any private keys held by it, as well as any passwords, passphrases, PINs or other secrets used in the course of carrying out its responsibilities as Registration Authority.

LSOM may, with the approval of LDRC, delegate a portion of its responsibilities under this Certificate Policy to LDRC, but remains responsible for ensuring that the delegated responsibilities are carried out in accordance with this Certificate Policy.

3.2 End-user Responsibilities

3.2.1 Subscriber's Responsibilities

It is the responsibility of a subscriber to:

(1) review the certificate issued to him or her to confirm the accuracy of the subscriber information contained in it before using it for the first time;

(2) use a trustworthy system for generating or obtaining a key pair and to prevent any loss, disclosure or unauthorized use of the private key;

(3) keep confidential his or her private key and any passwords, passphrases, PINs or other secrets used to obtain authenticated access to the LDRC/LSOM PKI facilities;

(4) make only true and accurate representations to LSOM and LDRC in support of an application for a certificate or for a renewal or reinstatement of a certificate;

(5) read the information provided to the subscriber regarding the use and security of the certificate and the associated key, and acknowledge his or her responsibilities regarding the use of a certificate under this Certificate Policy;

(6) use the certificate only for legal purposes authorized by this Certificate Policy (section 1.4); and

(7) immediately cease to use his or her certificate and notify LDRC, in accordance with the procedures set out in this Certificate Policy, when:

(a) the subscriber knows or suspects that his or her private key has been compromised; or

(b) any change occurs that adversely affects the subscriber's eligibility for, or the validity of, the subscriber's certificate.

3.2.2 Relying Party's Responsibilities

It is the responsibility of a relying party to:

(1) restrict reliance on a certificate issued under this Certificate Policy to appropriate uses of the certificate (section 1.4);

(2) before relying on a certificate, verify that the certificate has not expired, and has not been revoked or suspended, by accessing the certificate status information in the repository; and

(3) before relying on a certificate, determine that the certificate provides adequate assurances for the particular use intended between the parties.

4. SUBSCRIBERS AND THEIR CERTIFICATES

4.1 Naming of subscribers

LDRC will assign to each subscriber a unique name that conforms to the X.500 Distinguished Name format. The Distinguished Name is published in the X.509 Subject name field.

A Distinguished Name has several attributes, including a Common Name, an Organization Name and a Serial Number. If possible, the Common Name of a subscriber who is a member of LSOM should be the name under which he or she is registered with LSOM. For any other subscriber, the Common Name should be the person's legal name. The Serial Number attribute will be assigned a Globally Unique Identifier (GUID) to ensure that no two individuals have the same Distinguished Name.

The attributes of a subscriber's Distinguished Name must be such as to enable LDRC (and in turn LSOM) to identify the subscriber. Anonymity and use of a pseudonym are not permitted.

Before assigning a name to a subscriber as requested by him or her, LDRC may require the subscriber to demonstrate his or her right to use that name. Information may be added to a subscriber's Distinguished Name to minimize confusion as to the identity of multiple subscribers with the same or similar Common Name attributes. In the event of a dispute regarding the name assigned or to be assigned to a subscriber, LDRC may alone or in consultation with LSOM make the final decision.

Trademark issues associated with the use of a name are outside the scope of this Certificate Policy.

4.2 Authentication of Subscriber's Identity

LSOM is responsible for maintaining a PKI database authenticating each subscriber who is a lawyer authorized to practice law in the Province of Manitoba and for authenticating or approving procedures for verification of any other subscriber or any relying party. The authentication procedures may include face-to-face authentication or any other procedures that LSOM determines in its discretion and that LDRC determines in its discretion to reliably certify that the subscriber is a member of the legal profession entitled to practice law in the Province of Manitoba and also is the person named in the certificate issued to the subscriber.

4.3 Replacement Certificates

4.3.1 Term of certificate (5 years)

A subscriber's certificate and the corresponding key-pair are normally valid for five years. However, where the subscriber is a lawyer entitled to practice law in the Province of Manitoba, they cease to be valid when the subscriber is no longer authorized to practise law in Manitoba.

4.3.2 Routine re-key (renewal before end of 5-year term)

Before a certificate's 5-year term expires, LDRC will notify the subscriber of the pending expiry date and ask the subscriber to confirm his or her wish to renew the certificate. If the subscriber responds in the affirmative before the expiry date and remains eligible for a certificate, authentication of the subscriber's identity is not required, and will issue a new certificate to the subscriber.

In these circumstances, the procedures for issuing a new certificate apply in respect of confirmations required from the subscriber.

4.3.3 Re-key to reflect modification

If a change in circumstances warrants a change in any information contained in a certificate, and the subscriber remains eligible for a certificate, LDRC will issue a new certificate provided the change of information does not also require modification of financial arrangements with the subscriber by virtue of a change of firm or other commercial change. Where a commercial change is involved, LDRC will facilitate a modified commercial status by notifying the subscriber of new requirements and providing any forms as soon as reasonably possible.

In these circumstances, the procedures for issuing a new certificate to a subscriber apply in respect of confirmations required from the subscriber.

4.3.4 Re-key after revocation

If a subscriber's certificate is revoked, the application and issuance procedures for a new certificate apply to the issuance of any certificate to be issued to the person whose certificate was revoked. LSOM may waive an application requirement if:

(1) the subscriber is temporarily unable to meet the requirement in person (for example, the subscriber is away on extended travel) and the revocation did not occur because of a private key compromise; or

(2) the certificate was revoked by LDRC for any reason not related to conduct of the subscriber or compromise of the subscriber's private key.

4.4 Revocation of Certificate

4.4.1 Circumstances for revocation

A certificate shall be revoked by LDRC whenever such revocation is directed by reference to the LSOM PKI database because the subscriber has ceased to be a lawyer entitled to practice law in the Province of Manitoba or has become subject to restrictions inconsistent with use of a certificate. A certificate shall also be revoked by LDRC whenever a subscriber has died or is sufficiently incapacitated that the subscriber unable to benefit further from the issuance of a certificate in the name of the subscriber or where there are reasonable grounds to believe that the certificate has been misused or that control of private keys has been compromised.

4.4.2 Who can request a revocation

Revocation can be requested by LSOM directly by notice to LDRC or by virtue of an update to the PKI database maintained by LSOM, by a law firm responsible for a subscriber member of the firm and for costs associated with use of a certificate or by the individual subscriber, or such subscriber's trustee or executor.

4.4.3 Revocation request procedure

Requests for revocation shall be made in writing, provided that requests for revocation may be made by e-mail where LDRC is satisfied with the legitimacy of the e-mail communication. A digitally signed email sent from the subscriber to LDRC or LSOM shall be deemed to be a legitimate e-mail communication in the absence of any report of compromise of private keys.

Revocation may also be requested by the subscriber appearing in person at the LSOM or LDRC office along with proof of identity.

5. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

5.1 Certificate Application

5.1.1 Who can submit a certificate application

Lawyers permitted to practice in Manitoba may submit a certificate application as well as other parties authorized by LSOM.

5.1.2 Enrollment process and responsibilities

The Enrollment Process:

(1) the applicant uses the LDRC form (provided on the LDRC website) to initiate the request;

(2) applications may be prepared by a law firm or Legal Aid Manitoba on behalf of a subscriber but the application must be countersigned by the subscriber;

(3) LDRC receives the application and in the case of lawyer applications to LDRC, LDRC authenticates the status of the subscriber using the LSOM PKI database or files with LSOM any supplementary paperwork required for certificate issuance;

(4) LDRC receives the fee, as applicable;

(5) LDRC issues a certificate including where applicable issuance to the subscriber of required software to generate key pairs and certificates or instructions to deliver individual key pairs;

(6) it is acknowledged that Legal Aid Manitoba will not use software supplied by LDRC to generate key pairs and will instead receive public and private key pairs generated by LDRC. Where a subscriber is an employee of Legal Aid Manitoba and provides a written consent, key pairs may be issued to the IT Manager of Legal Aid Manitoba in trust for the subscriber.

LSOM Responsibilities:

(1) for lawyer applicants, LSOM maintains a database to verify the entitlement of the subscriber to receive a certificate and digital signature as a lawyer entitled to practice in Manitoba;

(2) LDRC confirms the identity of the subscriber based on procedures approved by LSOM;

(3) where subscribers other than lawyers have been authorized by LSOM, LDRC shall follow identity verification procedures agreed upon by LSOM and LDRC.

Applicant Subscriber Responsibilities:

(1) provide required information on the application;

(2) understand the information relating to the use and security of the certificates and the associated keys.

Accepted Subscriber Responsibilities:

(1) protect the private keys associated with all certificates held from unauthorized access;

(2) understand the information relating to the use and security of the certificates and the associated keys and accept individual subscriber responsibilities associated with use of a certificate particularly legal responsibilities associated with its use including the inability to repudiate consequence of use as outlined in this Certificate Policy;

(3) immediately cease to use the digital signature and key pairs and notify LDRC of any change of subscriber status resulting from a change of employer or another change which may affect the validity of the certificates held;

(4) notify LDRC and LSOM of any suspected or confirmed compromise of private keys;

(5) use the digital signature and public and private keys only for the purposes provided for in this Certificate Policy.

5.1.3 Eligibility

The following persons are eligible for a certificate:

(1) a lawyer authorized to practise law in Manitoba;

(2) relying parties identified by LDRC and approved by LSOM; and

(3) other specific persons or classes of persons based on eligibility criteria and class definitions published by LDRC following approval by LSOM.

5.1.4 Certificate Application

An applicant for a certificate must:

(1) use the application form and procedures approved by LDRC and available on the LDRC website or by link from the LSOM website;

(2) pay the fee, if any, payable to LDRC for the application;

(3) if the key-pair is generated by the applicant's cryptographic module, or by a key generator that transfers the key to the module, prove possession of the private key;

(4) if the key pair is delivered, prove possession of the private key and confirm the identity of any other party with access to it;

(5) complete an application form supplied by LDRC, addressed to LDRC and available to LSOM:

(a) attesting to the access restrictions to the private key for signing, or encrypting and signing, documents;

(b) providing any other assurances required by LDRC from time to time; and

(6) incorporating an undertaking of the subscriber to assume full legal responsibility for the subscriber's digital signature being attached to any document.

LDRC must verify the identity of lawyer applicant by reference to LSOM data and check all subscriber information provided in the application. If satisfied that the applicant is eligible for a certificate, LDRC shall issue the certificate to the applicant, and notify the applicant accordingly.

5.1.5 Obtaining and proving possession of private key

If the key-pair is generated directly by the applicant's cryptographic module, or a key generator that transfers the key to the applicant's cryptographic module, then the applicant is considered to possess the private key when it is generated or transferred. Possession may be proved by using that key to digitally sign the application for the certificate.

If the applicant is not in possession of the cryptographic module when the key-pair is generated, then the cryptographic module and activation data or key-pairs must be delivered to the applicant using a secure and accountable method that ensures that the private key is delivered to the applicant and that any other person with access to such private key is explicitly identified and provides suitable assurance(s) to LDRC with respect to the security of the private key. LDRC must keep a record validating the applicant's receipt of the cryptographic module and activation daa and any applicable information concerning delivery of key pairs and other parties with access to them. If a mechanism is used to share a password, pass-phrase or other secret information required to use the activation data to generate a certificate, the mechanism must ensure that the only recipients of the information are LDRC and the applicant.

All subscribers who are lawyers will acknowledge the following provision of the Code of Professional Conduct adopted by the LSOM as part of the subscription agreement:

> **Electronic Registration of Documents**
>
> **5.01 (5)** A lawyer who has personalized encrypted electronic access to any system for the electronic submission or registration of documents must not:
>
> (a) permit others, including a non-lawyer employee, to use such access; or
>
> (b) disclose his or her password or access phrase or number to others.

5.01 (6) When a non-lawyer employed by a lawyer has a personalized encrypted electronic access to any system for the electronic submission or registration of documents, the lawyer must ensure that the non-lawyer does not:

(a) permit others to use such access; or

(b) disclose his or her password or access phrase or number to others.

5.1.6 Authorized use of private key by person other than subscriber

LDRC will obtain written permission from LSOM before allowing any person other than the subscriber to use the subscriber's private key. At such time as such permission has been obtained, the application for permission should be supported by:

(1) an undertaking of the other person acceptable to LDRC and to LSOM if that becomes a term of the permission granted to LDRC by LSOM;

(2) insurance or a bond in favour of LDRC, and also in favour of LSOM if applicable, to insure against damages arising from unauthorized or improper use of the private key; and

(3) an undertaking of the subscriber to assume full legal responsibility for the subscriber's digital signature being attached to any document whether it was applied with or without the subscriber's authorization.

5.2 Certificate Application Processing

5.2.1 Identification and authentication functions

LDRC will identify lawyer applicant subscribers in accordance with Section 4.1 of this Certificate Policy. For other applicants authorized by LSOM, LDRC will follow identification procedures agreed upon by LSOM and LDRC.

5.2.2 Approval or rejection of certificate applications

LDRC will approve a certificate application if:

(1) all required documents and required fees have been received;

(2) it is satisfied with the documentation and verified the eligibility of the subscriber to hold a certificate; and

(3) it has verified the identity of the subscriber.

5.2.3 Time to process certificate applications

Once all required documents and fees have been received and any identification issues resolved, LDRC shall process the application and either issue a certificate together with required software or key pairs or reject the application, within 10 business days.

5.3 Certificate Issuance

5.3.1 LDRC actions during certificate issuance

When LDRC receives authorization from LSOM PKI database to issue one or more certificates, it shall provide software to the subscriber capable of generating required key pairs as instructed and create and sign the associated certificates. Where provision of software is impractical as described in section 4.12 (6), LDRC shall internally generate key pairs and follow the procedures outlined in section 4.12. Prior to delivery, LDRC shall also securely retain any private keys generated directly in accordance with Section 4.12 (6) of this Certificate Policy. LDRC shall in all cases also ensure it receives confirmation of the subscriber generation of key pairs and the subscriber's undertaking to protect such subscriber's private key. All certificate and key generation shall be logged.

5.3.2 Notification to subscriber by LDRC of issuance of certificate

Once all actions under Section 4.3.1 are satisfactorily completed, LDRC shall notify the subscriber by e-mail that the certificates have been issued.

5.4 Certificate Acceptance

5.4.1 Conduct constituting certificate acceptance

Before a subscriber is issued a certificate and associated keys, LDRC shall:

(1) confirm the identity of the recipient in accordance with Section 4.2;

(2) require the subscriber to indicate acceptance of all obligations and the subscriber's certificate, with either a previously issued digital or a handwritten signature; and

(3) document the subscriber's acceptance of responsibilities and the subscriber's certificate.

Once the above has been completed the subscriber will be deemed to have accepted the certificate.

5.4.2 Publication of the certificate by LDRC

Accepted Certificates and associated public keys shall be published by LDRC in accordance with this Certificate Policy.

5.4.3 Notification of certificate issuance by LDRC to other entities

LDRC may notify other entities including particularly relying parties of accepted Certificates under the terms of an agreement with them.

5.5 Key Pair and Certificate Usage

5.5.1 Subscriber private key and certificate usage

A subscriber shall use certificates only for lawful and authorized intended purposes as listed in Section 1.4 of this Certificate Policy. Unless special written authorization has been obtained from LSOM and LDRC, only the subscriber may use the private key associated with the certificate and, notwithstanding such special authorization, such subscriber will continue to be fully responsible for all such subscriber's certificate usage for any permitted purpose.

5.5.2 Relying party public key and certificate usage

A relying party shall use certificates only for lawful and authorized intended purposes as listed in Section 1.4 of this Certificate Policy. The relying party is responsible for confirmation of the status of the certificate with LDRC as a condition of placing reliance on it but may otherwise rely on the certificate as certifying the certified document was issued or issued and signed, as applicable, by the subscriber to whom the certificate was issued.

5.6 Certificate Renewal

5.6.1 Circumstance for certificate renewal

A certificate may be renewed prior to its expiry in exceptional circumstances where a re-key is not appropriate, provided that where the subscriber is a lawyer, that subscriber is still entitled to practice law in the Province of Manitoba and is not subject to any restrictive conditions inconsistent with use of such a certificate.

5.6.2 Who may request renewal

The subscriber, or where applicable, the subscriber's law firm, may initiate a request through LDRC to renew a certificate and extend its life based on exceptional circumstances, or LSOM may request a renewal and an extension of the life of a certificate on behalf of the subscriber from LDRC, on its own initiative, in similar exceptional circumstances, where a re-key is not appropriate.

5.6.3 Processing certificate renewal requests

Renewals follow the same process as applications for new certificates but may require completion of renewal forms.

5.6.4 Notification of new certificate issuance to subscriber

Same as for a new certificate.

5.6.5 Conduct constituting acceptance of a renewal certificate

Same as for a new certificate as set out in 5.4.1.

5.6.6 Publication of the renewal certificate by LDRC

Same as for a new certificate as set out in 5.4.2.

5.6.7 Notification of certificate issuance by the CA to other entities

Same as for a new certificate as set out in 5.4.3.

5.7 Certificate Re-key

5.7.1 Circumstance for certificate re-key

A certificate re-key may take place if the certificate or its associated private key is revoked due to compromise but the subscriber remains eligible to receive and use a certificate.

5.7.2 Who may request certification of a new public key

The subscriber or a subscriber's law firm may initiate a request through LDRC.

5.7.3 Processing certificate re-keying requests

Re-key requests follow the same process as new certificates but may use different application or request forms.

5.7.4 Notification of new certificate issuance to subscriber

Same as for a new certificate as set out in 5.3.2.

5.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as for a new certificate as set out in 5.4.1.

5.7.6 Publication of the re-keyed certificate by the CA

Same as for a new certificate as set out in 5.4.2.

5.7.7 Notification of certificate issuance by the CA to other entities

Same as for a new certificate as set out in 5.4.3.

5.8 Certificate Modification

5.8.1 Circumstance for certificate modification

A certificate modification may take place if the subscriber's name or law firm changes or other information alters the certificate processes or contents, other than the unique public and private key, but the subscriber remains eligible to hold the certificate.

5.8.2 Who may request certificate modification

The subscriber or the subscriber's law firm may initiate a request through LDRC.

5.8.3 Processing certificate modification requests

Modification requests follow the same process as new certificates as set out in section 5.1.4, but may use a different application or request form.

5.8.4 Notification of new certificate issuance to subscriber

Same as for a new certificate as set out in 5.3.2.

5.8.5 Conduct constituting acceptance of a modified certificate

Same as for a new certificate as set out in 5.4.1.

5.8.6 Publication of the modified certificate by LDRC

Same as for a new certificate as set out in 5.4.2.

5.8.7 Notification of certificate modification by LDRC to other entities

Same as for a new certificate as set out in 5.4.3.

5.9 Revocation

5.9.1 Circumstances for revocation

Certificates issued to users will be revoked before the expiration of the certificate validity period in the following circumstances:

(1) *A subscriber voluntarily leaves practice*. All certificates issued to the subscriber will be revoked within 30 days of leaving practice unless practice authorized by LSOM is resumed within that period.

(2) *A subscriber has made such subscriber's password for such subscriber's certificate available to another person in contravention of Section 5.1.5.* Unless special written authorization has been obtained from LSOM and LDRC, only the subscriber may use the private key associated with the certificate. Notwithstanding such special authorization, such subscriber will continue to be fully responsible for all such subscriber's digital signatures used for any permitted purpose

(3) *A subscriber is disbarred.* All certificates issued to such subscriber will be immediately revoked following disbarment.

(4) *A subscriber chooses not to renew such subscriber's practicing certificate (including failure to pay fees).* All certificates issued to the subscriber will be revoked within 30

days of receipt of notice by LDRC from LSOM based on an update of the LSOM PKI database unless the subscriber is reinstated prior to revocation.

(5) *A subscriber is suspended from practicing law*. All certificates issued to the subscriber will be revoked immediately following any suspension unless the subscriber is reinstated by LSOM by an update of the LSOM PKI database maintained by LSOM or LDRC receives special authorization to maintain the certificate from LSOM.

(6) *A subscriber takes a disability or other extended leave of absence*. All certificates issued to the subscriber must be immediately revoked if the subscriber does not return to work within 12 months.

(7) *A subscriber dies*. All certificates issued to the subscriber must be revoked immediately.

(8) *Reorganization of a firm or law practice.* If a firm or law practice is reorganized into a new entity that changes its name, the certificates issued may be revoked if LDRC or LSOM believes certification responsibilities will be compromised by the change; however, in such circumstances LDRC will both attempt to maintain as much continuity as possible so long as LDRC and, where required, LSOM, agree that continuity is consistent with ensuring equivalent legal responsibility in the course of such change.

(9) *A computer is lost or stolen.* If a computer is lost or stolen and one or more subscriber's private keys were on the computer, all certificates issued to the applicable subscriber(s) must be immediately revoked.

(10) *The CERTIFICATION AUTHORITY is compromised.* If the CERTIFICATION AUTHORITY (CA) computer is compromised, all certificates issued by that CA are considered compromised. The CA certificate must be revoked.

(11) *A cryptographic module is lost or stolen*. If a cryptographic module is found to be missing, the subscriber must notify the LSOM and LDRC that the cryptographic module is missing. When notice is received, the associated certificate(s) must be suspended immediately. If the cryptographic module is not recovered within 10 days, or if it is found to have been out of the control of the subscriber, the applicable certificate must be revoked.

(12) *Suspected private key compromise.* All certificates issued to such subscriber will be immediately revoked following suspected key compromise. Depending on the circumstances, a new certificate may be issued to the subscriber in the discretion of LDRC or issuance of a new certificate may be denied because of inappropriate safeguarding of a previously issued certificate or certificates.

5.9.2 Who can request revocation

(1) the subscriber may request revocation;

(2) LSOM may indirectly instruct LDRC by an update to the PKI database maintained by LSOM to revoke a subscriber's certificate if it becomes aware of any of the circumstances in Section 4.9.1 involving the subscriber or the certificate; or

(3) LDRC may revoke subscriber certificates or its own certificates if LDRC becomes aware of any of the circumstances in Section 4.9.1 which involve a subscriber's certificate or LDRC certificates.

5.9.3 Procedure for revocation request

(1) The subscriber may request revocation by sending a digitally signed e-mail to LSOM or LDRC requesting revocation.

(2) LSOM may request revocation by updating its PKI database accordingly or by sending a digitally signed e-mail to LDRC requesting revocation.

(3) LDRC may revoke its subscriber(s) or its own certificates unilaterally.

5.9.4 Revocation request grace period

Where a revocation notice is accompanied by a request for a grace period, LDRC may permit a grace period up to 48 hours following receipt of an appropriate request.

5.9.5 Time within which LDRC must process the revocation request

LDRC must process a revocation request absent a grace period request as fast as possible and in any event within 48 hours of an unqualified revocation request.

5.9.6 Revocation checking requirement for relying parties

All relying parties will automatically check LDRC's current Certificate Revocation List (CRL), which CRLs will be posted to the LDRC notice server and reflected in the validation procedures for the certificates. Revoked certificates will not be functional following validation. In the event of any outage, copies of CRLs will be sent by e-mail to any relying party requesting a copy of the CRL. In these circumstances, if an application is unable to obtain revocation information, the application may be set to accept or reject the certificate, depending upon the agreement between LDRC and any applicable relying party, until such time as the authenticity of the certificate can be determined.

5.9.7 Certificate Revocation List (CRL) issuance frequency

CRLs will be periodically issued and posted to the LDRC server, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which LDRC should appropriately post early updates, as described in this Certificate Policy. LDRC shall also ensure that a superseded CRL is removed from the server repository upon posting of the latest CRL, following which procedure, a revoked certificate is to be no longer trusted.

5.9.8 Maximum Latency for CRLs

CRLs will be published on the LDRC website within 24 hours of notification by the LSOM PKI database that a certificate has been revoked and applicable certificates will be revoked on the PKI validation site interim the same period.

5.9.9 On-line revocation/status checking availability

A CRL will be published on the LDRC notice server accessible through the LDRC website and will be accessed by the Entrust PKI for validation purposes. OCSP is not explicitly supported but is not required in this case for validation purposes.

5.9.10 On-line revocation checking requirements

None stipulated.

5.9.11 Other forms of revocation advertisements available

None.

5.9.12 Special requirements re key compromise

A subscriber who has reason to suspect that a private key held by him/her has been compromised shall request revocation without delay.

5.9.13 Circumstances for suspension

See Section 4.9.1.

5.9.14 Who can request suspension

See Section 4.9.2.

5.9.15 Procedure for suspension request

See Section 4.9.3.

5.9.16 Limits on suspension period

See Section 4.9.1.

5.10 Certificate Status Services

5.10.1 Operational characteristics

The CRLs for certificates issued under this Certificate Policy shall be posted on the LDRC notice server accessible through the LDRC website and and subscriber certificates shall be accessible through the Entrust PKI client software provided to subscribers. CRLs will be signed by LDRC for authenticity verification.

5.10.2 Service availability

The LDRC notice server and LDRC website operate 24x7 absent scheduled and unscheduled outages. Service bulletins for scheduled outages shall be posted on the LDRC website and shall take place out of normal business hours.

5.10.3 Optional features

No stipulation.

5.11 End of Subscription and Termination

5.11.1 End of Subscription

A subscriber may end a subscription by requesting revocation of all current certificates or allowing all certificates to expire without renewal. However, the contractual and other elements of subscription in accordance with this Certificate Policy, will not end until after all certificates issued to the subscriber have also expired.

5.11.2 CA or RA Termination

In the event that the LDRC CA operation is no longer possible or feasible, LDRC CA operation may, with the agreement of LDRC and LSOM be transferred to LSOM or another entity. If that is not agreed upon LDRC CA operations may be terminated. The preferable method is to terminate services at the same time as the certificates expire. If this is not possible, all certificates will be revoked and the CRL will be made available for as long as practical. In either event, an effort will be made to give relying parties as much notice as possible of the relocation or cessation of CA services. LSOM will be the custodian of archived records of CA operations.

LSOM will not terminate its role as Registration Authority unless its legislation is changed to prevent it from fulfilling that role or it is advised by its insurer or determines that continuation in such a capacity would be imprudent; in the latter event LDRC may determine that it is prepared to assume the legal responsibilities associated with acting as Registration Authority or to make arrangements with another party including a relying party or parties to assume that role, in which case the LDRC CA operations may continue.

5.12 Key Escrow and Recovery

5.12.1 Key escrow and recovery policy and practices

Key escrow is not explicitly supported. If directed by a court order or statutory provision, LDRC on its own or in consultation with LSOM may direct recovery or recover a subscriber's decryption key. Where any such court order is issued so directing LDRC or any statutory provision is invoked and applied to LDRC, LDRC shall immediately give notice to LSOM and LDRC shall not take any steps to recover a subscriber's decryption key except where required to do so by law or after reasonable notice to LSOM or, where LSOM confirms that it is not pursuing a court challenge or dispute resolution process in advance of LDRC surrendering the decryption key.

5.12.2 Session key encapsulation and recovery policy and practices

Session key encapsulation and recovery is not supported.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The Root CA signing key pair was created during the root key generation process for the LDRC CA, is protected by a cryptographic module generated as part of the root key generation process, and shall be retained at a location removed from the LDRC CA system data centre.

For all subscriber certificates, PKI software or a cryptographic module generates the key pairs. For an encryption certificate, the private key is securely stored in the CA database.

6.1.2 Private key delivery to Subscriber

The subscriber key pair will be generated by software delivered to the subscriber by LDRC after installation on a subscriber computer. The certificate is delivered to the user only after validation of the identity of the subscriber at the time of installation and through the LDRC/LSOM PKI database based on the requirements in this Certificate Policy.

6.1.3 Public key delivery to certificate issuer

The PKI software generates the key pairs for almost all users and no delivery is required. Where operating system and applications limitations prevent operation of such PKI software, key pairs may be generated at LDRC's office and shall thereafter be hand delivered to a trusted person acting on behalf of the subscriber as described in sections 3.3.3 and 5.1.2. No further delivery is required.

6.1.4 CA public key delivery to relying parties

The CA verification public key is available on the LDRC website. It is delivered as a PKCS#12 or PKCS#7 file with the complete chain of certificates that include the public keys, thus providing the trust validation tree.

6.1.5 Key sizes

(1) Subscriber signing key pairs are 1024 RSA.

(2) Subscriber authentication key pairs are 1024 RSA.

(3) Subscriber encryption key pairs are 1024 RSA.

(4) Root CA key pair is 2048 RSA.

(5) CA signing key pairs are 2048 RSA.

6.1.6 Public key parameters generation and quality checking

LDRC uses software to generate the subscriber keys. The software generates cryptographically secure key pairs. In other cases, keys will be delivered to a trusted person on behalf of the subscriber and tested by the subscriber in conjunction with LDRC immediately following delivery. The CA keys were generated and tested as part of the CA root key generation process.

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

See section 7 for key usage as per Section 7.1.1 base certificates and 7.1.2 certificate extensions.

The LDRC CA private key will be used only for signing the LDRC CA certificate, CRLs and in an extraordinary circumstance where a certificate may be required for test purposes.

Subscriber certificates may have one or more of the following Extended Key Usage values included:

(1) digitalSignature;

(2) nonRepudiation;

(3) keyEncipherment;

(4) DataEncipherment;

(5) secureEmail;

Where the digitalSignature key usage bit is included, the nonRepudition Key usage bit shall also be used.

6.2 Private Key Protection

6.2.1 Cryptographic module standards and controls

The cryptographic module used to generate keys on the CA server shall comply with FIPS 140-2 Level 2.

6.2.2 Private key (n out of m) multi-person control

These actions must be authorized by two persons who are CA Administrators or Certificate Managers.

(1) Creating new CA certificates.

(2) Change to existing CA certificates.

(3) Renewing CA certificates.

(4) Backing up CA private key material.

6.2.3 Private key escrow

Private key escrow is not explicitly supported. If directed by a court order or statutory provision or by LSOM, LDRC may direct recovery or recover a subscriber's decryption key. Where any such court order is issued against LDRC or any statutory provision is invoked and applied to LDRC, LDRC shall immediately give notice to LSOM and except where ordered to do otherwise or required to do otherwise by statute, LDRC shall not take any steps to recover a subscriber's decryption key except after 48 hours notice to LSOM or LSOM confirms that it is not pursuing a court challenge or dispute resolution process in advance of LDRC surrendering the decryption key. Where LSOM declines to take any action, LDRC may, but is not required to, engage its own counsel to review any such order or statutory provision and challenge same in an appropriate circumstance.

6.2.4 Private key backup

CA databases are backed up at a minimum on a daily basis and no private key escrow or backup is maintained.

Subscriber private decryption keys are backed up in the PKI database and LDRC thereby retains the ability to suspend operation of a subscriber's key pairs while retaining the ability to decrypt previous message traffic. Only a Certificate Manager can extract the encrypted private key from the CA database.

Recovery requests for private keys may be made by the subscriber to LDRC or may be requested through LSOM and any recovery will then be directed to LDRC for action. LDRC will not independently act upon a recovery request.

6.2.5 Private key archival

The encryption key pair history for all PKI users, including a complete history of all decryption private keys is stored in encrypted form in the PKI database.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

CA digital signature key storage shall be kept on a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

6.2.8 Method of activating private key

Any user must be explicitly authenticated to the cryptographic module before the activation of the private key. A private signing key must be authenticated each time it is used. This

authentication, at a minimum, will be in the form of a password. LDRC may also implement token based, or other authentication models in its discretion.

6.2.9 Method of deactivating private key

For the LDRC CA, when keys are deactivated the application must clear the keys from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity. The cryptographic module must automatically deactivate a private signing key after each use.

6.2.10 Method of destroying private key

For the LDRC CA, all sensitive keys in memory are overwritten with zeros when no longer used. Permanent destruction of private keys shall be completed with secure deletion operations from all locations.

For the LDRC CA, private keys shall be destroyed when they are no longer needed, meaning after a reasonable time following expiry or revocation of the certificates to which they correspond as determined by the board of LDRC. For software cryptographic modules, this will be completed by overwriting the data. For hardware modules, this will be completed by executing a "zeroize" command or other similar secure deletion. Physical destruction of hardware is not contemplated.

6.2.11 Cryptographic module rating

All LDRC CA digital signature key generation, CA digital signature key storage and certificate signing operations shall be performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 2.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The LDRC CA shall retain all verification public keys as required by statute and other agreements. The minimum period shall be 10 years after expiry of the public key.

6.3.2 Usage periods for the public and private keys

The following lifetimes are defined for the LDRC CA hierarchy:

(1) Root CA: CA signing key lifetime is set to twenty years.

(2) Subscriber Certificates and the associated keys have a maximum of five years.

6.4 Activation Data

6.4.1 Activation data generation and installation

All access to LDRC PKI CA components is managed by passwords or pass-phrases. They are required by all parties logging on to PKI components. For subscribers, passwords are selected by the subscriber for subscriber keys and by the appropriate LDRC CA person for CA keys.

The rules for password selection are:

(1) It must have at least eight characters including at least one digit.

(2) It must have at least one upper-case letter.

(3) It must have at least one non-alpha or non-numeric key.

(4) It must have at least one lower-case letter.

(5) It must not have been used in the last 24 months.

(6) It must not be the same as another password in use by the same subscriber (subscribers may be asked to confirm same).

6.4.2 Activation data protection

In addition to the above rules, subscribers will be responsible for ensuring activation data is protected against disclosure based on instructions provided by LDRC.

6.4.3 Other aspects of activation data

None.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Computing devices and software used for LDRC CA operations shall be selected with consideration to their roles and shall be maintained and patched as required.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

System hardware and software components shall be obtained from reputable sources.

6.6.2 Security management controls

Security auditing, log analysis and other tools shall be used to verify the correct operation of the CA system.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network Security Controls

The LDRC CA network shall use adequate firewalls and other network security elements to protect the online components of the CA system from compromise. The root signing key shall not be present on any device connected to a network.

6.8 Time-stamping

All certificates and certificate related entries in the LDRC CA database are time-stamped based on the clock setting of the device which performed the time-stamping. Certificate Managers shall maintain the accuracy of those clocks. All time-stamps shall include time and date and specify the time zone.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The CA shall issue X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile.

7.1.2 Certificate extensions

(1) authorityKeyIdentifier: Contains the key identifier of the issuing CA's public key (SHA1);

(2) KeyUsage: As specified in Section 6.1.7;

(3) certificatePolicies: Certificate policy OID = OID;

(4) subjectAlternativeName: Alternative name of the same subject;

(5) BasicConstraints: optional;

(6) CRL Distribution Points: URI to CRL distribution point (LDAP and/or HTTP).

7.1.3 Algorithm Object Identifiers

Algorithm Name	Object Identifier
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Name forms

In general, the Distinguished Name will be the full name of the subscriber. Some applications may require one or more alternative name formats. In this case, an alternate name form may be included in the subjectAlternativeName extension.

7.1.5 Name constraints

Cross CA certificates issued to partner organizations shall impose name constraints and path length constraints as defined in the PKI agreement with the partner organization.

7.1.6 Certificate policy object identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

LDRC will not issue certificates with policy qualifiers.

7.1.9 Processing semantics for the critical certificate policies extension

The PKI client applications must process extensions in accordance with PKIX Part 1.

7.2 CRL Profile

This CA and its subsidiaries issue X.509 Version 3 CRLs in accordance with IETF RFC 5280.

7.2.1 Version number(s)

The CRL version is set to v3.

7.2.2 CRL and CRL entry extensions

Version 3 CRL, and CRL extensions and their current status are specified below:

(1) CRLNumber: Populated by the CA application;

(2) reasonCode: Populated by the CA application as specified by operator;

(3) authorityKeyIdentifier: Populated by CA application with the key id (SHA1) of issuer public key.

7.3 OCSP Profile

The LDRC CA does not support the Online Certificate Status Protocol.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER AUDIT ASSESSMENTS

8.1 Frequency or circumstances of assessment

An audit of the LDRC PKI operations is performed annually.

8.2 Identity/Qualifications of Auditor

The auditor shall:

(1) have a demonstrated understanding of cryptography, TCP/IP networking, relational databases and web server technology;

(2) have a demonstrated understanding of policies, procedures and general security practices for IT systems and for PKI implementations; and

(3) possess a suitable professional designation.

8.3 Auditor's Relationship to Audited Party

The auditor shall not be:

(1) a member of the board or of the staff of LDRC;

(2) an immediate relative of a member of the board or of the staff of LDRC; or

(3) a person who otherwise may be perceived as being biased in the performance of the audit.

8.4 Topics Covered by Audit

The annual audit investigates the operations of the CA and RA functions of the LDRC PKI to ensure their compliance with this Certificate Policy and with other applicable PKI procedures. Some areas of focus for these audits may include, but are not limited to:

(1) management of the service, e.g., subscriber authentication and registration, security administration access control, configuration management, exception reporting and review, contingency planning;

(2) operations, e.g., trouble calls, system backup;

(3) software functionality, e.g., key management;

(4) hardware platform, e.g., secure operating system, robustness; and

(5) physical security, e.g., computer room access.

8.5 Actions Taken as a Result of Deficiency

There are two possible actions to be taken as a result of identification of a deficiency:

(1) continue to operate subject to any modification agreed upon by LDRC and LSOM; or

(2) suspend operation.

If a deficiency is identified, appropriate representatives of LDRC and LSOM will determine whether it is appropriate to modify procedures or operations and whether a suspension of operations is required. Depending on the severity of the deficiency, LDRC will consult its auditor concerning suitable means of correction.

If a deficiency is noted but operation of the CA continues, LDRC is responsible for ensuring that corrective actions are taken within 30 days from final issuance of the report. At that time, or earlier if agreed by both LDRC and LSOM, the auditor will reassess the deficiency. If, upon reassessment, corrective actions have not been taken or have not remedied the deficiency, appropriate representatives of LDRC and LSOM will determine what further action to take.

If operation is suspended, all certificates issued by LDRC, including subscriber certificates and CA cross-certificates, may be revoked prior to suspension of the service if LDRC and LSOM representatives feel that action is warranted. Upon reassessment, if the deficiencies are deemed to have been corrected, LDRC will resume service and new certificates to replace any which were revoked will be issued to PKI subscribers and any other applicable parties including external relying parties as required.

8.6 Communication of Results

Results of the annual audit are provided to the CEO of LSOM and the President of LDRC. If service is suspended, LDRC and LSOM will ensure all PKI subscribers and relying parties are informed of the action. Communication may be performed via email.

Relying party and other agreements set up with business partner organizations may also dictate that such parties are informed of any deficiencies. Unless specified in a particular relying party or other agreement, no communication of the audit results will occur outside LDRC and LSOM.

Should external relying parties or other parties need to be informed, LDRC will communicate the necessary information to the contact point specified in the applicable contracts.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Term and Termination

9.1.1 Term

This document becomes effective when first published on the LDRC website.

9.1.2 Termination

This document terminates when CA operations terminate in accordance with Section 4.11.2.

Changes may be made at any time and will become effective when published on the LDRC website.

9.1.3 Effect of termination and survival

In spite of termination of the LDRC CA, the Sections of this Certificate Policy respecting confidentiality and protection of private information together with any intellectual property rights associated with this Certificate Policy remain in effect.

9.2 Individual Notices and Communications with Participants

Notices from LDRC to subscribers, relying parties and other participants shall be either in writing with a specimen signature or by digitally signed e-mail and return communications shall take place in the same form. If communication is to be by digitally signed e-mail, the parties shall first agree in writing to communicate by signed e-mail and establish e-mail addresses to be used for the purpose.

9.3 Amendments

9.3.1 Procedure for amendment

LDRC may review this Certificate Policy at any time and shall review it at least once every year. LSOM may also review this Certificate Policy at any time that it becomes aware of a change, such as a change in a statute, regulation or operational procedure that may render the contents or utility of this Certificate Policy inappropriate in the circumstances. Errors, updates, or suggested changes to this document shall be communicated to the contacts specified in the Contact Details section of this Certificate Policy. Such communication must include a detailed description of any proposed change, a change justification, and contact information for the person requesting the change.

The LDRC President and LSOM Chief Executive Officer must approve all changes to this Certificate Policy. In the course of determining whether to give such approval, those parties may

engage other persons or entities as required for the evaluation of the changes and the effect of changes on subscribers, Relying Parties and other participants in the LDRC PKI.

9.3.2 Notification mechanism and period

If a material change in this Certificate Policy is required, a notice will be given to the subscribers and relying parties by posting same on the LDRC websites and, at the option of such parties, by notice inserted into publications read by members of the legal community. Except in the case of changes deemed urgent by such LDRC and LSOM personnel, a period of 30 days will be allowed for comments to be received from participants before making the change effective.

9.3.3 Circumstances under which OID must be changed

If a policy change is determined by LDRC and LSOM personnel reviewing this Certificate Policy to require the issuance of a new policy, LDRC will obtain a new OID for the new policy from the appropriate authority.

9.4 Financial Responsibilities

9.4.1 Limited Liability of Trust Service Providers

By signing a certificate that identifies the use of this Certificate Policy, LDRC and LSOM certify to all government and Court relying parties specifically engaging with LDRC to use such certificates and who reasonably rely on the information contained in the certificate that the certificate holder is eligible to practice law in the Province of Manitoba and that application and subscriber information has been provided and checked according to the procedures set out in this Certificate Policy.

As stated in the LDRC Subscriber Agreement:

(1) neither LDRC nor LSOM assumes any liability whatsoever in relation to the use of a certificate or the associated keys for any use other than in accordance with this Certificate Policy. A subscriber who uses a certificate or the associated keys for any other purpose must indemnify LDRC and LSOM against any liability, costs and claims arising from that use;

(2) neither LDRC nor LSOM is liable for any consequential, indirect or incidental damages, or for any loss of business or profit, whether foreseeable or unforeseeable, however arising from or in relation to the use of, or reliance on, any digital certificate in accordance with this Certificate Policy, unless it is directly attributable to its negligence or wilful misconduct;

(3) neither LDRC nor LSOM is liable to an end user in contract, in tort (including negligence) or otherwise for any act or omission of any provider of a telecommunication or Internet service for any fault in or failure of their equipment.

9.4.2 Responsibility of Subscriber and Indemnification by Subscriber of Relying Party for unauthorized use

Subscribers are bound by the restrictions applicable to the use of certificates and their corresponding keys issued under this Certificate Policy. A subscriber who uses a certificate or an associated key for any other purpose must indemnify LDRC and LSOM against any liability, costs and claims arising from that use.

Unless special written authorization has been obtained from LSOM and LDRC, only the subscriber may use the private key associated with the certificate and, notwithstanding such special authorization, such subscriber will continue to be fully responsible for all such subscriber's digital signatures used for any permitted purpose. A subscriber who permits use of a certificate or an associated key by another person must indemnify the relying party, LDRC and LSOM, against any liability, costs and claims arising from that use.

9.4.3 No fiduciary relationship

Neither LDRC nor LSOM is, by virtue of this Certificate Policy or any service provided under it, an agent, fiduciary, trustee or other representative of a subscriber or other relying party. No subscriber or other relying party has any authority to bind LDRC or LSOM, by contract or otherwise, to any obligation.

9.5 Notice Provisions

Whenever any subscriber hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by paper-based communications. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgement of receipt from recipient. Such acknowledgement must be received within five (5) working days, or else notice must then be given by paper-based communications. Such paper-based communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed to LDRC as detailed in section 1. All such communications shall be effective upon receipt.

A subscriber requiring receipt of notice under this Certificate Policy is required to provide notice of:

(1) changes in address including postal and email addresses;

(2) changes in financial or other status, which would change the basis upon which the Certificate has been granted; and

(3) any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

Notice may be given to Relying Parties by digitally signed or unsigned messages, or by making such notice accessible online in a similar manner as that used for the publication of this Certificate Policy.

Notice requirements with regard to termination of LDRC CA operations are specified in section 9.1.2 and 9.2.

Notice requirements with regard to changes in this Certificate Policy are specified in section 9.1.2.

9.6 Fees - Principles

9.6.1 Fees will be set by LDRC to permit recovery of costs to establish itself as a Certificate Authority and to cover general overhead on a not-for-profit basis. Subscribers will be notified of fees in the subscriber agreement or in notices provided by LDRC from time to time. Fees may be determined based on different service choices or purposes of a subscriber and may be transaction based.

9.6.1 Certificate Issuance or Renewal Fees

LDRC may charge a fee for the issuance and renewal of certificates. The board of LDRC shall set the fee from time to time.

9.6.2 Certificate Access Fees

LDRC may charge a fee for access to certificates. The board of LDRC shall set the fee from time to time.

9.6.3 Revocation or Status Information Access Fees

LDRC may charge a fee for revocation or status information, including access to CRLs. The board of LDRC shall set the fee from time to time.

9.6.4 Fees for Other Services

LDRC may charge a fee for other services, such as policy information and software licences. The board of LDRC shall set the fee from time to time.

9.6.5 Refund Policy

The board of LDRC may establish a policy governing refunds of fees which is not inconsistent with this Certificate Policy.

9.7 Financial Responsibility

9.7.1 Insurance coverage

LDRC shall maintain appropriate insurance coverage for its liabilities including any liabilities to relying parties or applicable parties.

9.7.2 Other assets

Not applicable.

9.7.3 Insurance or warranty coverage for end-entities

LDRC shall maintain appropriate insurance coverage for its liability to end-entities.

9.8 Confidentiality of Business Information

9.8.1 Scope of confidential information

All information relating to LDRC's activities when acting as a CA, unless exempted by Sections 5.3.2, 5.9.6, 5.9.7 or other specific provisions of this CP, including but not limited to, business plans, sales information, trade secrets, organizational name, registration information, financial information, technical information, licence agreements and agreements with any other PKI relying parties or participants, shall be considered confidential information.

9.8.2 Information not within the scope of confidential information

Any and all information made public in a certificate issued by LDRC acting as a CA or published in a CRL shall not be considered confidential.

9.8.3 Responsibility to protect confidential information

Any participants that receive confidential information are to secure it from compromise, and refrain from using it or disclosing it to third parties except as provided by law. All contractors or other temporary participants shall agree be bound by the provisions of this Certificate Policy by a Non-disclosure Agreement.

If directed by a court order or statutory provision or by LSOM, LDRC may direct recovery or recover a subscriber's decryption key or provide other confidential information to parties LDRC is directed to supply with such information pursuant to such court order or statutory provision. Where any court order is issued against LDRC or any statutory provision is invoked and applied to LDRC, LDRC shall immediately give notice to LSOM and except where ordered to do otherwise, LDRC shall not take any steps to recover a subscriber's decryption key except after 48 hours notice to LSOM or LSOM confirms that it is not pursuing a court challenge or dispute resolution process in advance of LDRC surrendering the decryption key. In all cases, LDRC shall take reasonable steps to ensure the protection of privileged information.

9.9 Privacy of Personal Information

In this section, Personal Information is defined as is it is in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000, c. 5.

9.9.1 Privacy plan

LDRC does not have a written privacy plan. LDRC policy, as directed by its Board, is not to disclose private personal information of its subscribers, customers, employees, partners, or other parties with whom it is engaged, without their prior written consent unless required by due process of law and, where possible, following consultation and review with LSOM.

9.9.2 Information treated as private

Any information about subscribers or other participants that is not made public through the certificates issued by this CA, or published in a CRL, is considered private information.

9.9.3 Information not deemed private

Any and all personal information made public in a certificate issued by LDRC acting as a CA or published in its CRL, shall not be considered private or confidential.

9.9.4 Responsibility to protect private information

LDRC will make reasonable commercial efforts with respect to private personal information to secure it from compromise, and refrain from using it or disclosing it to third parties except as required by law. LDRC will also ensure that contracts signed with contractors or other parties who may have access to private information contains suitable protections and non-disclosure provisions.

Any relying or other party that receives private personal information will also be required to comply with PIPEDA and its Regulations and to any provincial statute that may apply with respect to the protection of privacy.

9.9.5 Notice and consent to use private information

Where LDRC is requested to provide private information by consent LDRC shall give appropriate notice to any subscriber and obtain a written consent from such subscriber before supplying such information except where LDRC is required by statute to supply such information without notice and consent.

9.9.6 Disclosure pursuant to judicial or administrative process

LDRC will disclose all private or other information required pursuant to judicial or administrative process provided that unless otherwise directed by a court order, LDRC will give immediate notice to LSOM and the subscriber of any direction or request of that nature and will follow any instructions given to it by LSOM to protect privilege. In the absence of a direction from LSOM, LDRC will take reasonable steps to ensure the propriety of any process other than a court order which would give rise to disclosure of private information of a subscriber. In all cases, LDRC shall take reasonable steps to ensure the protection of privileged information.

9.9.7 Other information disclosure circumstances

None.

9.10 Intellectual Property Rights

Certificates and CRLs issued by LDRC when acting as a CA are the property of LDRC and LSOM.

The Distinguished Names used to represent entities under this Certificate Policy are the property of LDRC.

With respect to the CA system, the software, including any related copyright, trademark, and patent rights, may be owned by software vendors and will remain the sole and exclusive property of those vendors subject to any proprietary rights LDRC may acquire by contract.

This Certificate Policy is the intellectual property of LDRC. LSOM is granted full use of this Certificate Policy with the exception of distribution for gain.

9.11 Representations and Warranties

9.11.1 CA representations and warranties

LDRC will operate the CA in accordance with this Certificate Policy.

Authentication will be implemented as set forth in Section 3 of this Certificate Policy.

Persons with defined PKI roles shall be individually accountable for their actions.

LDRC will take reasonable steps to make subscribers and relying parties aware of their respective rights and obligations with respect to their use of and reliance upon any keys, and/or certificates used in connection with the LDRC PKI. To the extent LDRC is in possession of private keys for any subscriber or relying party or other party, LDRC shall take reasonable commercial steps to ensure private keys are safeguarded as described in and required by this CSP.

9.11.2 RA representations and warranties

No stipulation.

9.11.3 Subscriber representations and warranties

No stipulation.

9.11.4 Relying party representations and warranties

No stipulation.

9.11.5 Representations and warranties of other participants

No stipulation.

9.12 Disclaimers of Warranties

LDRC does not warrant that the information in the certificates issued by it is consistent with the information which was provided by the subscriber to LDRC or LSOM, merely that by inclusion of a subscriber's name in its PKI database LSOM has authorized LDRC to issue a Certificate to a subscriber.

Nothing contained in this document shall create any fiduciary relationship between LDRC and a subscriber or relying party or other participant in the PKI or confer authority on any such party to act for or on behalf of LDRC in any capacity.

9.13 Limitations of Liability

Provided that LDRC has fulfilled the requirements of this Certificate Policy, LDRC will not assume liability for any damages to any participant including a subscriber, Relying Party or any other party arising out of or related to the use of, or reliance upon keys and/or certificates issued by LDRC acting as a CA that are or have been:

(1) revoked;

(2) expired;

(3) used for a purpose outside the scope of purposes permitted herein;

(4) used by other than the authorized subscriber or relying party;

(5) altered;

(6) compromised;

(7) fraudulently obtained; or

(8) become the subject of any misrepresentation, misleading act or omission.

9.14 Indemnities

Except as otherwise provided by this Certificate Policy and/or a Subscriber Agreement, LDRC's contracts with all subscribers and/or relying parties will include terms requiring such parties to indemnify and hold harmless LDRC and LSOM from any and all claims, actions or demands that result from the use of a key or the use or publication certificate when a claim arises from:

(1) any false or misleading statement made by a subscriber;

(2) any deceptive act by a subscriber;

(3) any failure on the part of a subscriber to properly protect a private key and/or cryptographic module;

(4) any failure on the part of a subscriber to promptly notify LDRC and LSOM of a suspected or actual compromise, disclosure, loss, or unauthorized use of the subscriber's private key once the subscriber has become aware of such an event; or

(5) any use of a private key by anyone other than its associated subscriber.

9.15 Dispute Resolution Provisions

In the event of any dispute, the matter in dispute shall be submitted to LDRC and LDRC in consultation with LSOM shall determine a dispute resolution method including mediation or informal or formal arbitration processes to which the parties shall submit. Where the dispute involves an action or inaction of LDRC, LDRC shall immediately refer the matter to LSOM which shall direct the process of dispute resolution to be followed.

9.16 Governing Law

This Certificate Policy shall be governed and interpreted according to the laws of Manitoba, Canada.

9.17 Compliance with Applicable Law

LDRC shall comply with applicable laws in Manitoba and Canada and may agree to be bound be applicable law in another jurisdiction where it deems such compliance to be appropriate. Agreements between LDRC and relying parties or other parties may contain provisions which address applicable law in the jurisdictions of the parties.

9.18 Miscellaneous Provisions

9.18.1 Entire agreement

Not applicable.

9.18.2 Assignment

Not applicable.

9.18.3 Severability

In the event that a court of competent jurisdiction or other administrative tribunal finds that any clause or section of this Certificate Policy is, for any reason, invalid or otherwise unenforceable, the remainder of the document shall remain in force. The same shall apply to any agreements or contracts between parties that include or refer to this Certificate Policy.

9.18.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.19 Other Provisions

None.