Bell Canada

Bell Root CA

Certificate Policy

Date:	January 25, 2008
Approved by:	
Version:	1.0

All Rights Reserved

© 2008 Bell Canada

REVISION HISTORY

Version	Description	Date Issued	Date Approved
1.0	First Release	Jan. 25, 2008	

© 2008 Bell Canada

TABLE OF CONTENTS

1. Introduction 5
1.1. Overview 5
1.2. Document Name and Identification 5
1.3. PKI Participants 5
1.4. Certificate Usage 6
1.5. Policy Administration 6
1.6. Definitions and Acronyms 6
2. Publication and Repository Responsibilities 9
3. Identification and Authentication (I&A) 10
3.1. Naming 10
3.2. Initial Identity Validation 10
3.3. Identification and Authentication for Re-key Requests 10
3.4. Identification and Authentication for Revocation Requests 10
4. Certificate Life-Cycle Operational Requirements 11
4.1. Certificate Application 11
4.2. Certificate Application Processing 11
4.3. Certificate Issuance 11
4.4. Certificate Acceptance 11
4.5. Key Pair and Certificate Usage 11
4.6. Certificate Renewal 11
4.7. Certificate Re-key 11
4.8. Certificate Modification 11
4.9. Certificate Revocation and Suspension 12
4.10. Certificate Status Services 12
4.11. End of Subscription 12
4.12. Key Escrow and Recovery 12
5. Facility, Management, and Operational Controls 13
5.1. Physical Security Controls 13
5.1.1 Site Location and Construction 13
5.1.2 Physical Access 13
5.1.3 Power and Air Conditioning 13
5.1.4 Water Exposure 13
5.1.5 Fire Prevention and Protection 13
5.1.6 Media Storage 13
5.1.7 Waste Disposal 13
5.1.8 Off-site Backup 14
5.2. Procedural Controls 14

5.3. Personnel Controls 14
5.4. Audit Logging Procedures 14
5.5. Records Archival 15
5.6. Key Changeover 15
5.7. Compromise and Disaster Recovery 15
5.8. CA or RA Termination 15
6. Technical Security Controls 16
6.1. Key Pair Generation and Installation 16
6.2. Private Key Protection and Cryptographic Module Engineering Controls 16
6.3. Other Aspects of Key Pair Management 17
6.4. Activation Data 17
6.5. Computer Security Controls 17
6.6. Life Cycle Security Controls 17
6.7. Network Security Controls 17
6.8. Timestamping 17
7. Certificate, CRL, and OCSP Profiles 18
7.1. Certificate Profile 18
7.2. CRL Profile 19
7.3. OCSP Profile 19
8. Compliance Audit and Other Assessment 20
9. Other Business and Legal Matters 21
9.1. Fees 21
9.2. Financial Responsibility 21
9.3. Confidentiality of Business Information 21
9.4. Privacy of Personal Information 21
9.5. Intellectual Property Rights 21
9.6. Representations and Warranties 21
9.7. Disclaimers of Warranties 22
9.8. Limitations of Liability 23
9.9. Indemnities 24
9.10. Term and Termination 24
9.11. Individual notices and communications with participants 24
9.12. Amendments 24
9.13. Dispute Resolution Procedures 24
9.14. Governing Law 24
9.15. Compliance with Applicable Law 25
9.16. Entire Agreement 25
9.17. Assignment 25
9.18. Force Majeure 25

1. Introduction

1.1. Overview

This document defines the digital signature Certificate Policy (CP), at Medium Assurance (as per Canadian government standards), for use in the Bell Root Certificate Authority (CA). This document follows and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

The Certificate Policy defined in this document is intended for use within Bell Canada and its subsidiaries. Users of this document are to consult the issuing CA to obtain further details of the implementation of this Certificate Policy.

This CP governs the management and use of certificates containing public keys used for verification mechanisms. Specifically, the certificates issued under these policies will be used for verifying the identity of subordinate CAs in Bell Canada.

The Subscriber has no authority to conduct business transactions on behalf of the organization operating the CA.

The CA will be governed by the laws of Canada and applicable provincial law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

Any exceptions to this CP must be approved in writing by the Bell PKI Governance Board.

Bell Canada reserves the right not to enter into a cross certification agreement with an external Certification Authority.

1.2. Document Name and Identification

bell-pki-certpcy-RootCA -digitalSignature ::= { ioint-iso-itut-t (2) country (16) Canada (124) Bell (113565) pki (3) CertificatePolicy (1) Root CA (1) DigitalSignature (1) }

1.3. PKI Participants

This policy recognizes the following participants:

- The CA, which signs and issues certificates
- The Registration Authority (RA), which is responsible for ensuring the legitimacy of requests for certificates
- Subscribers, which will be subordinate CAs
- Relying Parties, which could be any person or entity, in Bell or outside, that seeks to verify the authenticity of a subordinate CA.

1.4. Certificate Usage

The certificates issued by a CA operating under this CP shall be used only by subordinate CAs. The subordinate CAs may use the certificates issued to them by the Bell Root CA only to sign the certificates they issue, or (after obtaining the approval of the Bell PKI Governance Board) to cross-certify a third party's CA.

1.5. Policy Administration

The organization responsible for drafting, registering, maintaining, and updating this Certificate Policy is the Bell PKI Governance Board, which can be contacted at bellpki@bell.ca.

1.6. Definitions and Acronyms

Term	Definition
Bell PKI Governance Board	The combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives.
Certificate Authority	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List	A list maintained by a Certification Authority of the certificates which it has issued that have been revoked prior to their stated expiration date.
Certification Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a CP, or requirements specified in a contract for services).
Distinguished Name	A set of attribute-value pairs that unique identifies an object within a given directory.
Hardware Security Module	A hardware device for securely generating and storing cryptographic keys.

© 2008 Bell Canada

Public Key Cryptography Standard #10 (PKCS#10)	The format for messages sent to a Certificate Authority to request certification of a public key.
Public Key Infrastructure	A set of policies, processes, server platforms and software used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Key Infrastructure X.509	The IETF standard (RFC 3280) that defines the format of a digital certificate.
Registration Authority	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Relying Party	Any person, computer or other entity that relies of the authenticity of the binding between the public key and the distinguished name in a digital certificate.

Acronym	**Explanation**
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority

© 2008 Bell Canada

RSA	Rivest-Shamir-Adleman

2. Publication and Repository Responsibilities

An issuing CA has responsibilities relating to the publication of the certificates it issues. It must:

- Ensure the publication of its CP on a web site accessible to all Relying Parties (the web site can be maintained by the CA or some other party on behalf of the CA, but the choice of web site must be approved by the Bell PKI Governance Board), once the CP has been approved by the Bell PKI Governance Board;
- Include within any certificate it issues the URL of the web site hosting the CP;
- Ensure that operating system and repository access controls will be configured so that only authorized CA personnel can write or modify the online version of the CP; and
- Provide a full text version of the CPS when necessary for the purposes of any audit, inspection, accreditation or cross-certification.

Access controls may be instituted at the discretion of the CA with respect to certificates or on-line certificate status (if the latter is provided as a service by the CA). Certificates must be published promptly upon acceptance. A CA must ensure, directly or with agreement with a repository, unrestricted access to CRLs.

3. Identification and Authentication (I&A)

3.1. Naming

The Root CA's signing certificate shall use "C=CA,O=Bell,OU=Bell Root CA" for the Subject Distinguished Name (DN). Certificates issued by the Bell Root CA shall be given unique and distinguishable Subject DNs, in accordance with PKIX Part 1, in the form of a non-blank X.501 printable String. Issued certificates' Subject DNs must have an association with the organizational name of the subordinate CA, and must be approved prior to issuance by the Bell PKI Governance Board.

3.2. Initial Identity Validation

The Bell Root CA shall issue a certificate to a subordinate CA only upon receipt of proper authorization from the Bell PKI Governance Board (see section 4.1), and its process must provide a High Assurance (not merely Medium Assurance) that a subordinate CA does in fact possess the private key corresponding to the public key that has been presented in a request.

The process must also provide a High Assurance that the certificate that the subordinate CA receives has in fact been issued by the Bell Root CA.

3.3. Identification and Authentication for Re-key Requests

Requests to re-key the signing certificate of a subscriber subordinate CA may be carried out only upon receipt of proper authorization from the Bell PKI Governance Board (see section 4.7). The new certificate must provide the same High Assurance of authenticity as described in section 3.2.

3.4. Identification and Authentication for Revocation Requests

Requests to revoke the signing certificate of a subscriber subordinate CA may be carried out only upon receipt of proper authorization from the Bell PKI Governance Board (see section 4.9). The revocation process must provide the same High Assurance of authenticity as described in section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

The request to have a subordinate CA's signing certificate signed by the Bell Root CA must be made using the processes described in the Bell PKI Governance Board Charter. Any Bell Tier B manager (Director Level) may submit a request to have a CA certified by the Bell Root CA.

4.2. Certificate Application Processing

Certificate applications must be processed in accordance with the Bell PKI Governance Board Charter.

4.3. Certificate Issuance

The process whereby the Bell Root CA issues certificates must provide a High Assurance of authenticity, as described in section 3.2.

4.4. Certificate Acceptance

A subordinate CA must express its intention not to accept a certificate issued to it by the Bell Root CA within one (1) business day. If the subordinate CA does not express the intention not to accept the certificate, the subordinate CA shall be considered as having accepted the certificate.

Once a certificate has been accepted, the Bell Root CA must ensure the certificate is published in a repository that will be accessible by all Relying Parties.

4.5. Key Pair and Certificate Usage

Subscribing subordinate CAs shall use the certificates issued by the Bell Root CA only for the purpose of signing the certificates that they issue or (after obtaining the written approval of the Bell PKI Governance Board) cross-certifying a third party's CA. Relying parties may use the certificates issued by the Bell Root CA only for the purpose of validating that the certificates they are relying on were in fact signed by the subordinate CA as claimed.

4.6. Certificate Renewal

Certificate Renewal requests must be made to the Bell PKI Governance Board, and must follow the same process as certificate applications (see section 4.1ff).

4.7. Certificate Re-key

Certificate Re-key requests must be made to the Bell PKI Governance Board, and must follow the same process as certificate applications (see section 4.1ff).

4.8. Certificate Modification

Certificate Modification is not supported by the Bell Root CA, and certificate modification requests will be treated as new certificate applications.

4.9. Certificate Revocation and Suspension

Certificate revocation and suspension requests must be approved by the Bell PKI Governance Board. The revocation process must provide a High Assurance of authenticity, as described in section 3.4. The Bell Root CA is responsible for ensuring that the revoked/suspended certificate is published in a CRL that will be accessible to all Relying Parties. Suspension requests must be published within two (2) business days of being approved, revocation requests within five (5) business days. The requirements for the contents of the CRL are given in section 7.2.

4.10. Certificate Status Services

The Bell Root CA must support an on-line CRL, which must be accessible to all Relying Parties. The Bell PKI Governance Board shall make the Service Level Agreement concerning the availability of the CRL available to any Relying Party on request.

4.11. End of Subscription

A subscribing subordinate CA that wishes to end their subscription must apply to the Bell PKI Governance Board. If the request is approved, then a quorum (see section 5.2) of the Bell Root CA's registrars must revoke the subordinate CA's signing certificate.

4.12. Key Escrow and Recovery

The Bell Root CA must not include any facility for key escrow or recovery of the certificates it issues.

5. Facility, Management, and Operational Controls

5.1. Physical Security Controls

The physical security controls of the space housing the Bell Root CA must comply with provisions of this Policy as well as with the relevant Bell Security Policies, Practices, Procedures and Standards, Government regulations and all applicable laws.

5.1.1 Site Location and Construction

The site location and construction of the facility housing the Bell Root CA, when combined with other physical security protection mechanisms such as guards and intrusion sensors, must provide Medium Assurance (as per Canadian government standards) that the Bell Root CA equipment and records are protected against unauthorized access.

5.1.2 Physical Access

The Bell Root CA's equipment must always be protected from unauthorized access, especially while the cryptographic module is installed and activated.

Physical access controls must be implemented so as to provide Medium Assurance (as per section 5.1.1) of protection against the risk of equipment tampering, even when the cryptographic module is not installed and activated.

Access to the Bell Root CA's equipment and cryptographic materials must be limited to specific trusted personnel.

5.1.3 Power and Air Conditioning

The facility that houses the Bell Root CA's equipment must be supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.4 Water Exposure

The Bell Root CA's equipment must be installed in such a way that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

An automatic fire extinguishing system must be installed in accordance with local policy and code.

5.1.6 Media Storage

Media must be stored to protect them from accidental damage (e.g. water, fire, electromagnetic). Media that contain audit, archive, or backup information must be duplicated and securely stored in a location separate from the Root CA as per section 5.1.8, employing media protection equal to that of the Bell Root CA's primary site.

5.1.7 Waste Disposal

Waste must be removed or destroyed.

Media used to store sensitive data must be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

System backups, sufficient to recover from system failure, must be made on a periodic schedule. A backup must be created and stored at a separate from the Bell Root CA's equipment location at a facility with physical and procedural controls equal to that of the Bell Root CA's primary site. The backup facility must be at least 100km away from the primary site.

5.2. Procedural Controls

The operation of the Bell Root CA must include the following roles:

- System administrators, who are responsible for maintaining the operating system and application software for the server that runs the CA application and also the servers that make up the repository (or repositories) for the certificates and CRLs issued by the Bell Root CA as well as this CP, the supporting CPS and any required supporting documentation. System administration tasks can be performed by any individual authorized system administrator: a quorum (unlike CA administrators and registrars) of more than one administrator is not required.
- CA administrators, who are responsible for generating the Bell Root CA's private key, and for authorizing registrars. Generating the Bell Root CA's private key must require the participation of all CA administrators; authorizing a registrar must require the participation of a quorum of at least three CA administrators.
- Registrars, who are responsible for signing certificates issued by the Bell Root CA, and hence, activating the Bell Root CA's private signing key. Activating the Bell Root CA's private signing key must require the participation of a quorum of at least three registrars.

CA administrators may also be registrars, however strict segregation of duties is required between system administrators on the one hand, and CA administrators and registrars on the other.

5.3. Personnel Controls

System administrators, CA administrators and registrars of the Bell Root CA must comply with all relevant Bell HR screening procedures, and must also pass a criminal background check before they are allowed to begin their duties.

System administrators, CA administrators and registrars must receive training on the operation of the software and hardware they need to perform their functions, and must be retrained for each major new release.

5.4. Audit Logging Procedures

Each time the Bell Root CA's private signing key is activated, the fact must be logged, along with the identities of the registrars who activated it, the purpose of the activation and the serial number and Subject DN of the affected certificate.

The activation log must be kept for the entire lifespan of the CA, and must be viewable only by the CA administrators, registrars and the system administrators of the Bell Root CA. The log shall be kept in such a way as to resist subsequent tampering (e.g. on a write-once medium, or with all entries digitally signed). The log must be backed up within twenty-four hours of each new entry, also in such a way as to resist tampering. The backup must be kept in a separate secure location as per section 5.1.

5.5. Records Archival

All certificate application data, including approvals, plus all audit records, must be archived for the lifespan of the CA, plus seven years. Access to the archive must be restricted to the CA application administrators and registrars.

5.6. Key Changeover

The procedures for a key changeover of the Bell Root CA are identical to the procedures for generating its keys at the start; see section 6.1. The old certificate shall not be revoked or removed from the repository unless the Bell PKI Governance Board rules that there is a significant risk that the old private key was compromised.

5.7. Compromise and Disaster Recovery

The Bell Root CA must have a Disaster Recovery Plan that will permit it to resume operations within thirty days of a disaster. Should a disaster or compromise occur, all Relying Parties must be notified. The Bell Root CA must then be redeployed as per section 6.6. If the private key has been compromised, then the old Bell Root CA signing certificate must be revoked, and a new key pair generated as per section 6.1.

5.8. CA or RA Termination

Upon termination of the Bell Root CA, all Relying Parties must be notified. The Bell PKI Governance Board then becomes custodian or any archived materials, for as long as it is necessary for them to be kept.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

The signing key pair of the Bell Root CA must be generated in a Hardware Security Module (HSM) used exclusively by the Bell Root CA. The HSM must be built to be tamper resistant, and to show evidence of tampering, and installed in compliance with Bell Canada Physical Security requirements. The key pair must be an RSA key of at least 4096 bits. The Bell Root CA's certificate must be flagged as to be used for digital signature only (see section 7.1). Once the signing key pair has been generated, it must be copied onto a back-up HSM that must thereafter be kept in a secure location as per section 5.1.

Subordinate CA key pairs, the public keys of which are to be incorporated into certificates to be issued by the Bell Root CA, must be generated on the subordinate CAs, and must be RSA keys of at least 2048 bits. The subordinate CA's public key must be communicated to the Bell Root CA as described in section 3.2. Certificates issued by the Bell Root CA must be flagged as to be used for digital signature only (see section 7.1) and communicated to relying parties and the certificate repository as described in sections 3.2 and 4.4.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Any activation or maintenance activity on the Bell Root CA's HSM must require the cooperation of a quorum (see section 5.2) of registrars, and must be carried out in a secure location. No single Bell Canada employee may possess all access control components that would allow him/her to access a cryptographic module individually. The Bell Root CA's private key must never be escrowed or archived (see section 6.1 for key pair backup requirements).

Destroying the Bell Root CA's private key must require the participation of a quorum of registrars. Removing the Bell Root CA's HSM from service must be performed in the presence of a quorum of registrars. When removed from service, all HSM tokens and keys must be destroyed.

The PINs used for activation of the Bell Root CA private key must be at least eight digits in length.

Cryptographic components shall be shipped and accepted securely, and investigated and tested to ensure the components have not been tampered with. The storage areas where HSMs are stored shall be sufficiently secure to ensure that they are not tampered with or used without authorization while in storage.

Repairs to the HSM that are performed on-site may only be performed in the presence of at least three registrars or CA administrators. HSM Tokens that have been subject to repair shall only be placed in service at Bell Canada PKI site upon certification from the vendor that the HSM functions as required, and that it is as if it were newly purchased.

The private keys of the subordinate CAs whose certificates are signed by the Bell Root CA must never be escrowed or archived.

6.3. Other Aspects of Key Pair Management

The lifespan of the signing certificate of the Bell Root CA shall be 20 years. The lifespan of the certificates issued by the Bell Root CA shall be 15 years.

6.4. Activation Data

Each registrar must have a PIN that is at least eight digits in length to activate their function on the hardware encryption module.

6.5. Computer Security Controls

The computer hosting the Bell Root CA shall be maintained in accordance with the relevant Bell Security Policies, Practices, Procedures and Standards for its platform, operating system and application software.

6.6. Life Cycle Security Controls

The computer hosting the Bell Root CA shall be deployed in accordance with the relevant Bell deployment practices. Operating system and software patches shall be installed in accordance with the relevant Bell Security Policies, Practices, Procedures and Standards.

6.7. Network Security Controls

The computer hosting the Bell Root CA must not be connected to any Internet Protocol (IP) network at any time.

6.8. Timestamping

The time service on the computer hosting the Bell Root CA must be maintained to no more than ten seconds drift from the Bell standard time servers.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

The profile of the signing certificate of the Bell Root CA must be as follows:

Field	Contents
Version	Version 3
Serial number	A value that is unique across all certificates issued by the Bell Root CA.
Signature algorithm identifier	SHA-1
Issuer DN	C=CA,O=Bell,OU=Bell Root CA
Valid from	The time and date the certificate was issued
Valid to	20 years after the "Valid from" date.
Subject DN	C=CA,O=Bell,OU=Bell Root CA
Key usage	Digital Signature
Basic constrains	CA:TRUE
Authority key identifier	The 160-bit SHA-1 hash of the Public Key of the Bell Root CA.
Subject key identifier	The 160-bit SHA-1 hash of the Public Key of the Bell Root CA.
Certificate policies	2.16.124.113565.3.1.1.1
CRL distribution points	The URL of the Bell Root CA's CRL

The profile for the certificates issued by the Bell Root CA must be as follows:

Field	Contents
Version	Version 3
Serial number	A value that is unique across all certificates issued by the Bell Root CA.

Signature algorithm identifier	SHA-1
Issuer DN	C=CA,O=Bell,OU=Bell Root CA
Valid from	The time and date the certificate was issued
Valid to	15 years after the “Valid from” date.
Subject DN	The approved DN of the subordinate CA
Key usage	Digital Signature
Basic constrains	CA:TRUE
Authority key identifier	The 160-bit SHA-1 hash of the Public Key of the Bell Root CA.
Subject key identifier	The 160-bit SHA-1 hash of the Public Key of the subordinate CA.
Certificate policies	2.16.124.113565.3.1.1.1
CRL distribution points	The URL of the Bell Root CA’s CRL

7.2. CRL Profile

The profile for the CRL issued by the Bell Root CA must be as follows:

Revocation List	**Contents**
Serial number	Serial number of the revoked certificate
Revocation date	Date of certification revocation
CRL reason code	Revocation reason – explanation

7.3. OCSP Profile

The Bell Root CA will not support OSCP.

© 2008 Bell Canada

8. Compliance Audit and Other Assessment

The Bell Root CA must be audited by Bell Internal Audits before commencing operations, and at least once per year thereafter. It can also be audited at any time at the discretion of the Bell PKI Governance Board.

The audit findings are to be presented to the Bell PKI Governance Board, but shall be made available to all Relying Parties. In the event that deficiencies are identified in an audit, the Bell Root CA is obliged within two weeks to submit a plan to the Bell PKI Governance Board that will address these deficiencies. If the Bell PKI Governance Board finds the risks unacceptable, it may require the Bell Root CA to cease operations, either until an acceptable level or risk is achieved, or permanently.

9. Other Business and Legal Matters

9.1. Fees

The Bell Root CA does not intend to charge fees to any Bell organization, but reserves the right to do so at its sole discretion at any time.

9.2. Financial Responsibility

The Bell Root CA accepts no financial responsibility of any kind.

Any party relying on this Certificate Policy (CP) ("Relying Party") is responsible for having its own comprehensive general liability insurance policy, covering bodily and personal injury, including death, and property damage, including loss of use resulting from such party's negligence.

9.3. Confidentiality of Business Information

Any confidential information communicated to the Bell Root CA (such as possible confidential information included with certificate application information, and confidential parts of the CPS) and information such as audit trail records, audit reports, security measures, and disaster recovery plans will be considered confidential and handled in accordance with the relevant Bell Security Policies and relevant privacy laws of Canada.

Subordinate CA's or any other Relying Party who may have access to or receive any of this confidential information shall secure all such information from unauthorized access, protect its confidentiality, and refrain from using or disclosing it to third parties.

9.4. Privacy of Personal Information

Any personal information collected by the Bell Root CA will be handled in accordance with the relevant Bell Security Policies and the relevant privacy laws of Canada.

Information included in certificates and Certificate Revocation Lists (CRLs) issued by the Bell Root CA shall not be treated as private.

9.5. Intellectual Property Rights

All intellectual property rights arising from the deployment of the Bell Root CA, including the CP, CPS, certificates, names, and keys, and any products or information developed under or pursuant to this CP, remain the property of Bell Canada.

9.6. Representations and Warranties

An RA who performs registration functions as described in this CP shall comply with the stipulations of this CP.

Each Subordinate CA subscribing to the Bell Root CA represents and warrants that it shall:

- Provide correct information to the Bell Root CA without errors, omissions, or misrepresentations;
- Request revocation of a certificate if a key is no longer needed, upon the compromise or suspected compromise of a key;
- Memorize and not record any passwords or PINs associated with accessing or using private keys or cryptographic tokens;

- Exercise diligence in protecting their private keys and cryptographic tokens at all times against loss, theft or tampering;
- Inform the Bell Root CA within 48 hours of a change to any information included in it's certificate or certificate application request;
- Inform the Bell Root CA within 24 hours of a suspected compromise of one or all of its private keys, activation data, security module or any passwords or PINs used to access its private keys or cryptographic tokens;
- Understand the basic principles of Public Key certificates and their use within the business application;
- Use certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of this CP and applicable laws;
- Only use certificates on behalf of the person, entity, or organization listed as the subject of the certificate; and
- Read, understand and abide by all the terms, conditions, and restrictions in this CP and any other agreement with the Bell Root CA.

Each Relying Party represents and warrants to the Bell Root CA that it:

- shall use certificates exclusively for legal and authorized purposes in accordance with applicable laws; and
- understands and acknowledges that it is relying on this CP at its own risk and that Bell CA shall not be liable for any reliance thereon.

The Bell Root CA warrants that it exercises all due care in to assure that the information in the certificates it issues is accurate. However, Bell Root CA makes no representations or warranties with respect to:

- The techniques used in the generation and storage of the Private Key corresponding to the Public Key in certificates, including, whether such Private Key has been compromised or was generated using sound cryptographic techniques;
- The reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing a certificate;
- Any software whatsoever; or
- Non-repudiation of any certificate or digital signature verified using a certificate, since determination of non-repudiation is a matter of applicable law.

9.7. Disclaimers of Warranties

The Bell Root CA disclaims any warranty that its certificates may be of use for any purpose other than the validation of the identity of the subordinate CA.

The Bell Root CA is not liable for loss:

- Incurred due to any Relying Party's default in obligations, loss of service due to war, natural disasters, strikes, lock-outs, labour disputes or other uncontrollable forces.
- Incurred between the time that a certificate is revoked and the next issuance of a Certificate Revocation List.
- Due to unauthorized use of certificates issued by the Subordinate CA.

- Due to use of certificates beyond the prescribed use defined by the CP under which the certificate is issued. Caused by fraudulent or negligent use of certificates and/or CRLs issued by the Subordinate CA.
- Due to disclosure of information contained within certificates and CRLs; and
- Incurred if not notified of revoked certificates. The Bell Root CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

9.8. Limitations of Liability

The Bell Root CA and its employees, directors or providers, expressly disclaim any liability of any kind to any Subordinate CA, relying party, or any other individual or entity arising from the use of or reliance upon its certificates or any services provided by the Bell Root CA in respect to certificates.

The term "Medium Assurance" is not intended to convey any representation or warranty as to the availability of CA services offered under the Bell Root CA. Bell Canada does not represent or warrant 100% availability offered under the Bell Root CA.

This CP also contains limited warranties and disclaimers of representations, warranties and conditions. Each Relying Party acknowledges that to the extent that its reliance on any certificate causes itself or third party damages, of any type, the Bell Root CA shall not be held liable whatsoever. Each Subordinate CA shall provide a notice of limited liability within each certificate.

The foregoing disclaimer of liability shall apply to any liability whether based in contract (including fundamental breach), tort (including negligence) or any other theory of liability and shall apply notwithstanding the failure of essential purpose of any limited remedy stated herein and even if the Bell Root CA has been advised of the possibility of those damages.

The Bell Root CA will not compensate anyone for losses resulting from inappropriate or fraudulent use of this Public Key Infrastructure. The Bell Root CA disclaims all liability of any kind arising from tort, contract or any other form of claim in relation to the exportation or importation of cryptography products by individuals or organizations in connection with the use of Bell Root CA services.

The Bell Root CA further disclaims all liability of any kind whatsoever for matters outside of its control including the availability or working of the Internet, or telecommunications or other infrastructure systems.

9.9. Indemnities

Each Subordinate CA assumes all risks and liability inherent to the performance of its obligations hereunder and those of its employees, subcontractors and agents and shall take all necessary measures to avoid any damage to the Bell Root CA and anyone else who may be effected by the obligations hereunder. To that effect, the Subordinate CA agrees to defend, fully indemnify and hold harmless the Bell Root CA and anyone else who may be effected by the obligations hereunder from and against any and all claims, demands, suits, actions, causes of action and/or liability, of any kind whatsoever, for damages, losses, costs and/or expenses resulting from (i) damages to persons or property, personal injury or death caused by the negligent or willful acts or omissions of the Subordinate CA, employees, subcontractors and agents arising in connection with this CP or service; and (ii) any and all breaches by Subordinate CA of any representations, warranties, covenants, terms and conditions enumerated in this CP that are part of the Subordinate CA's responsibilities.

9.10. Term and Termination

This CP shall remain in force as long as the Bell Root CA continues to operate. Sections 9.3 , 9.8 and 9.9 shall survive termination of this CP.

9.11. Individual notices and communications with participants

Participants in and Relying Parties on this CP can communicate officially with the Bell Root CA by sending an e-mail to bellrootca@bell.ca.

9.12. Amendments

This CP can be amended only by approval of the Bell PKI Governance Board. This board is also responsible for deciding if an approved change changes the acceptability of the certificates issued under it to a degree that warrants changing the CP OID.

9.13. Dispute Resolution Procedures

A dispute concerning key and certificate management among entities in Bell shall be resolved, as a last resort, by the Bell PKI Governance Board. A dispute between Bell and an external entity that cannot be settled through negotiation or mediation shall be resolved through arbitration in accordance with the Commercial Arbitration Act of Canada.

9.14. Governing Law

The laws of Ontario and the federal laws of Canada applicable therein, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of this CP, and any agreements entered into by the CA. Any dispute in respect to this CP or agreement, or in respect to certificates or any services provided by the Bell Root CA in respect to certificates which is not resolved by alternative dispute resolution, shall be brought in the courts of the Province of Ontario, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes.

9.15. Compliance with Applicable Law

Participants in the Bell Root CA must comply with all applicable laws, ordinances, codes and regulations of governmental agencies including federal, provincial, municipal and local governing bodies having jurisdiction over the services provided hereunder, including, without limitation, those in respect of the treatment of cryptographic hardware and software.

9.16. Entire Agreement

This CP and the documents it references comprise the entire Certificate Policy of the Bell Root CA and constitute the entire agreement between the Subordinate CA and the Bell Root CA with respect to this subject matter, merging and superseding any previous statements or understandings concerning the Bell Root CA.

Should it be determined that any part of this CP is incorrect or invalid, the rest of the CP shall remain in effect and valid.

9.17. Assignment

Certificates and the rights granted under this CP or any agreement are specific to the Subordinate CA to whom a certificate was issued, and to the person, entity, or organization which entered into the agreement with the Bell Root CA, and cannot be assigned, sold, transferred, or otherwise disposed of, whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of the Bell Root CA.

Any attempted assignment or transfer without such consent shall be void and shall automatically terminate such Subordinate CA's rights under this CP or any Subscriber Agreement. The Bell Root CA may assign, sell, transfer, or otherwise dispose of this CP, or any agreement together with all of its rights and obligations under this CP and any agreements to an affiliate.

9.18. Force Majeure

The Bell Root CA shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or comply with the terms of this CP, any agreement, or any settlement amounts arising out of or related to delays in performance or from failure to perform due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, or the public enemy, riots and insurrections, war, terrorism, epidemics, accidents, fire, strikes and other labor difficulties, embargoes, judicial action, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.