Canada Revenue Agency

Agence du revenu du Canada

X 509 Public Key Infrastructure Certificate Policy for Person Entity

Version: 5.0
Date: 2019/05/10

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR	COMMENTS
0.1	Nov. 25, 2018	L. Chen	Initial draft
0.2	April 18, 2019	L. Chen	Minor adjustments to formatting
0.3	April 29, 2019	K. Chau	Formatting and updating some information
1.0	May 7, 2019	K. Chau	Update the document with the date of ITSC director approval
5.0	May 10, 2019	K. Chau	Update version number to align with previous document

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 OVERVIEW 1
1.1.1 Relationship between CP and CPS 1
1.1.2 Subordinate CA 1
1.1.3 Cross Certification 1
1.2 NAME AND IDENTIFICATION 2
{JOINT-ISO-ITU-T(2) COUNTRY(16) CA(124) GC(101) GCORG(1) CRA (272) CERTPCY(3) CERTIFICATES (#) PERSONUSER(1) CERTIFICATE(#)} 2
1.3 PKI PARTICIPANTS 2
1.3.1 Certification Authorities 2
1.3.2 Registration Authorities 3
1.3.3 Subscribers 3
1.3.4 Relying Parties 4
1.3.5 Other Participants 4
1.4 CERTIFICATE USAGE 5
1.4.1 Appropriate Certificate Uses 6
1.4.2 Prohibited Certificate Uses 6
1.5 CERTIFICATE POLICY ADMINISTRATION 7
1.5.1 Organization Administering the Document 7
1.5.2 Contact Information 7
1.5.3 Person Determining CPS Suitability for the Policy 7
1.5.4 CPS Approval Procedures 7
1.6 DEFINITIONS AND ACRONYMS 7
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 16
2.1 REPOSITORIES 16
2.2 PUBLICATION OF CERTIFICATION INFORMATION 16
2.2.1 Publication of Certificates and Certificate Status 16
2.2.2 Publication of CA Information 16
2.3 TIME OR FREQUENCY OF PUBLICATION 16
2.4 ACCESS CONTROLS ON REPOSITORIES 16
3 IDENTIFICATION AND AUTHENTICATION 18
3.1 NAMING 18
3.1.1 Types of Names 18
3.1.2 Need for Names to be Meaningful 18
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Various Name Forms 18
3.1.5 Uniqueness of Names 18
3.1.6 Recognition, Authentication and Role of Trademarks 18
3.2 INITIAL IDENTITY VALIDATION 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of an Organization Identity 19
3.2.3 Authentication of an Individual Identity (Identity Proofing) 20
3.2.4 Non-Verified Subscriber Information 21
3.2.5 Validation of Authority 21
3.2.6 Criteria for Interoperation 21
3.3 3.3 IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS 21
3.4IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 22
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 22

4.1 CERTIFICATE APPLICATION 23
4.1.1 Who Can Submit a Certificate Application 23
4.1.2 Enrolment Process and Responsibilities 23
4.2 CERTIFICATE APPLICATION PROCESSING 23
4.2.1 Performing Identification and Authentication Functions 23
4.2.2 Approval or Rejection of Certificate Applications 24
4.2.3 Time to Process Certificate Applications 24
4.3 CERTIFICATE ISSUANCE 24
4.3.1 CA Actions During Certificate Issuance 24
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 24
4.4 CERTIFICATE ACCEPTANCE 24
4.4.1 Conduct Constituting Certificate Acceptance 24
4.4.2 Publication of the Certificate by the CA 25
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 25
4.5 KEY PAIR AND CERTIFICATE USAGE 25
4.5.1 Subscriber Private Key and Certificate Usage 25
4.5.2 Relying Party Public Key and Certificate Usage 25
4.6 CERTIFICATE RENEWAL 25
4.6.1 Circumstances for Certificate Renewal 25
4.6.2 Who May Request Renewal 25
4.6.3 Processing Certificate Renewal Requests 25
4.6.4 Notification of New Certificate Issuance to Subscriber 26
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 26
4.6.6 Publication of the Renewal Certificate by the CA 26
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 26
4.7 CERTIFICATE RE-KEY 26
4.7.1 Circumstances for Certificate Re-Key 26
4.7.2 Who May Request Certification of a New Public Key 27
4.7.3 Processing Certificate Re-Keying Requests 27
4.7.4 Notification of New Certificate Issuance to Subscriber 27
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 27
4.7.6 Publication of the Re-Keyed Certificate by the CA 27
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 27
4.8 CERTIFICATE MODIFICATION 27
4.8.1 Circumstances for Certificate Modification 27
4.8.2 Who May Request Certificate Modification 27
4.8.3 Processing Certificate Modification Requests 27
4.8.4 Notification of New Certificate Issuance to Subscriber 27
4.8.5 Conduct Constituting Acceptance of a Modified Certificate 27
4.8.6 Publication of the Modified Certificate by the CA 27
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 28
4.9 CERTIFICATE REVOCATION 28
4.9.1 Circumstances for Revocation 28
4.9.2 Who Can Request Revocation 28
4.9.3 Procedure for Revocation Request 28
4.9.4 Revocation Request Grace Period 29
4.9.5 Time Within Which CA Must Process the Revocation Request 29
4.9.6 Revocation Checking Requirement for Relying Parties 29
4.9.7 CRL Issuance Frequency (if applicable) 29
4.9.8 Maximum Latency for CRLs (if applicable) 30

4.9.9 On-line Revocation/Status Checking Availability 30
4.9.10 On-line Revocation Checking Requirements 30
4.9.11 Other Forms of Revocation Advertisements AVAILABLE 30
4.9.12 Special Requirements re Key Compromise 30
4.9.13 Circumstances for Suspension 31
4.9.14 Who can Request Suspension 31
4.9.15 Procedure for Suspension Request 31
4.9.16 Limits on Suspension Period 31
4.10 CERTIFICATE STATUS SERVICES 31
4.10.1 Operational Characteristics 31
4.10.2 Service Availability 31
4.10.3 Optional Features 32
4.11 END OF SUBSCRIPTION 32
4.12 KEY ESCROW AND RECOVERY 32
4.12.1 Key Escrow and Recovery Policy and Practices 32
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 32
5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 33
5.1 PHYSICAL CONTROLS 33
5.1.1 Site Location and Construction 33
5.1.2 Physical Access 33
5.1.3 Power and Air Conditioning 34
5.1.4 Water Exposures 34
5.1.5 Fire Prevention and Protection 34
5.1.6 Media Storage 34
5.1.7 Waste Disposal 34
5.1.8 Off-site Backup 35
5.2 PROCEDURAL CONTROLS 35
5.2.1 Trusted Roles 35
5.2.2 Number of Persons Required per Task 37
5.3 PERSONNEL CONTROLS 38
5.3.1 Qualifications, Experience, and Clearance Requirements 38
5.3.2 Background Check Procedures 38
5.3.3 Training Requirements 39
5.3.4 Retraining Frequency and Requirements 39
5.3.5 Job Rotation Frequency and Sequence 39
5.3.6 Sanctions for Unauthorized Actions 39
5.3.7 Independent Contractor Requirements 39
5.3.8 Documentation Supplied to Personnel 39
5.4 AUDIT LOGGING PROCEDURES 39
5.4.1 Types of Events Recorded 39
5.4.2 Frequency of Audit Log Processing 43
5.4.3 Retention Period for Audit Log 44
5.4.4 Protection of Audit Log 44
5.4.5 Audit Log Back-up Procedures 44
5.4.6 Audit Collection System (Internal vs External) 44
5.4.7 Notification of Event Causing Subject 44
5.4.8 Vulnerability Assessments 44
5.5 RECORDS ARCHIVAL 45
5.5.1 Types of Records Archived 45
5.5.2 Retention Period for Archive 45

5.5.3 Protection of Archive 45
5.5.4 Archive Backup Procedures 46
5.5.5 Requirements for Time-Stamping of Records 46
5.5.6 Archive Collection System (Internal or External) 46
5.5.7 Procedures to Obtain and Verify Archive Information 46
5.6 KEY CHANGEOVER 46
5.7 COMPROMISE AND DISASTER RECOVERY 46
5.7.1 Incident and Compromise Handling Procedures 46
5.7.2 Computing Resources, Software and/or Data Are Corrupted 47
5.7.3 Business Continuity Capabilities After a Disaster 47
5.8 CA OR RA TERMINATION 48
6 TECHNICAL SECURITY CONTROLS 49
6.1 KEY PAIR GENERATION AND INSTALLATION 49
6.1.1 Key Pair Generation 49
6.1.2 Private Key Delivery to Subscriber 50
6.1.3 Public Key Delivery to Certificate Issuer 50
6.1.4 CA Public Key Delivery to Relying Parties 50
6.1.5 Key Sizes 51
6.1.6 Public Key Parameters Generation and Quality Checking 52
6.1.7 Key Usage Purposes (as per x.509v3 keyUsage field) 52
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 52
6.2.1 Cryptographic Module Standards and Controls 52
6.2.2 Private Key (n out of m) Multi-person Control 53
6.2.3 Private Key Escrow 54
6.2.4 Private Key Back-up 54
6.2.5 Private Key Archival 54
6.2.6 Private Key Transfer Into or From a Cryptographic Module 54
6.2.7 Private Key Storage on Cryptographic Module 55
6.2.8 Method of Activating Private Key 55
6.2.9 Method of Deactivating Private Key 55
6.2.10 Method of Destroying Private Key 55
6.2.11 Cryptographic Module Rating 55
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 55
6.3.1 Public Key Archival 55
6.3.2 Certificate Operational Periods and Key Usage Periods 55
6.4 ACTIVATION DATA 56
6.4.1 Activation Data Generation and Installation 56
6.4.2 Activation Data Protection 56
6.4.3 Other Aspects of Activation Data 56
6.5 COMPUTER SECURITY CONTROLS 56
6.5.1 Specific Computer Security Technical Requirements 56
6.5.2 Computer Security Rating 57
6.6 LIFE CYCLE TECHNICAL CONTROLS 57
6.6.1 System Development Controls 57
6.6.2 Security Management Controls 57
6.7 NETWORK SECURITY CONTROLS 58
6.8 TIME-STAMPING 58
7 CERTIFICATE, CRL AND OCSP PROFILES 59
7.1 CERTIFICATE PROFILE 59

7.1.1 Version Number(S) 59
7.1.2 Certificate Extensions 59
7.1.3 Algorithm Object Identifiers 59
7.1.4 Name Forms 60
7.1.5 Name Constraints 60
7.1.6 Certificate Policy Object Identifier 60
7.1.7 Usage of Policy Constraints Extension 61
7.1.8 Policy Qualifiers Syntax and Semantics 61
7.1.9 Processing Semantics for Critical Certificate Extensions 61
7.2 CRL PROFILE 61
7.2.1 Version Number(S) 61
7.2.2 CRL and CRL Entry Extensions 61
7.3 OCSP PROFILE 61
7.3.1 Version number 61
7.3.2 OCSP Extensions 61
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 62
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 62
8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR 62
8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY 62
8.4 TOPICS COVERED BY ASSESSMENT 62
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 63
8.6 COMMUNICATION OF RESULTS 63
9 OTHER BUSINESS AND LEGAL MATTERS 64
9.1 FEES 64
9.1.1 Certificate Issuance or Renewal Fees 64
9.1.2 Certificate Access Fee 64
9.1.3 Revocation or Status Information Access Fees 64
9.1.4 Fees for Other Services 64
9.1.5 Refund Policy 64
9.2 FINANCIAL RESPONSIBILITY 64
9.2.1 Insurance Coverage 64
9.2.2 Other Assets 64
9.2.3 Insurance or Warranty Coverage for End-Entities 64
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 65
9.3.1 Scope of Confidential Information 65
9.3.2 Information Not Within the Scope of Confidential Information 65
9.3.3 Responsibility to Protect Confidential Information 65
9.4 PRIVACY OF PERSONAL INFORMATION 65
9.4.1 Privacy Plan 65
9.4.2 Information Treated as Private 65
9.4.3 Information Not Deemed Private 66
9.4.4 Responsibility to Protect Private Information 66
9.4.5 Notice and Consent to Use Private Information 66
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 66
9.4.7 Other Information Disclosure Circumstances 66
9.5 INTELLECTUAL PROPERTY RIGHTS 66
9.6 REPRESENTATIONS AND WARRANTIES 67
9.6.1 CA Representations and Warranties 67
9.6.2 RA Representations and Warranties 68
9.6.3 Subscriber Representations and Warranties 69

9.6.4 Relying Party Representations and Warranties 69
9.6.5 Representations and Warranties Of Other Participants 70
9.7 DISCLAIMERS OF WARRANTIES 71
9.8 LIMITATIONS OF LIABILITY 72
9.9 INDEMNITIES 72
9.10 TERM AND TERMINATION 72
9.10.1 Term 72
9.10.2 Termination 72
9.10.3 Effect of Termination and Survival 73
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 73
9.12 AMENDMENTS 73
9.12.1 Procedure for Amendment 73
9.12.2 Notification Mechanism and Period 73
9.12.3 Circumstances Under Which OID Must be Changed 73
9.13 DISPUTE RESOLUTION PROVISIONS 73
9.14 GOVERNING LAW 74
9.15 COMPLIANCE WITH APPLICABLE LAW 74
9.16 MISCELLANEOUS PROVISIONS 74
9.16.1 Entire Agreement 74
9.16.2 Assignment 74
9.16.3 Severability 74
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 74
9.16.5 Force Majeure 74
9.17 OTHER PROVISIONS 74
APPENDIX 1 - REFERENCES 75

TABLE OF TABLES

Table 1: CRA PKI Certificate TYPE Names and Corresponding OIDs..2
Table 2: Certificate usage..5
Table 3: General Definitions 7
Table 4: Acronyms 13

1 INTRODUCTION

This policy takes effect on May 7th, 2019. It was approved by François Viens, Director of the IT Security Centre Division. François is also the CRA representative at the TBS' PKI Policy Management Authority (PMA).

This policy applies to Canada Revenue Agency and Canada Border Services Agency within the meaning of the *Financial Administration Act* (*FAA*) (Reference A), unless excluded by specific acts, regulations or Orders in Council.

This document is consistent with RFC3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Reference B)* from the Internet Engineering Task Force (IETF).

1.1 OVERVIEW

This document defines user certificates at the "protected" level for use by people working for or with the Canada Revenue Agency (CRA) and Canada Border Services Agency (CBSA). This CP identifies four discrete types of certificates aligned with the *Standard on Identity and Credential Assurance* (Reference C). These are the same levels as internationally standardized in the International Standard detailing the "*Entity authentication assurance framework*" (Reference H).

All certificates issued under this CP are intended for the use of the person to whom the certificate was issued (with the exception of group certificates, which are managed by the Group Custodian for which do not have digital signature or non-repudiation assurance).

Certificates issued under this Certificate Policy may be issued to:

a) CRA and CBSA employees (via Internal CA);
b) employees of other governments or international organizations; or
c) individuals of organizations having contractual relationships with the CRA and/or CBSA (via External CA).

1.1.1 RELATIONSHIP BETWEEN CP AND CPS

This CP states what identity assurance can be relied upon from a certificate issued by the Certificate Authority (CA). The Certificate Practice Statement (CPS) states how the CA establishes that assurance thru compliance with the CP. Each CA that issues certificates under this CP shall have a corresponding CPS.

1.1.2 SUBORDINATE CA

At the management authority's discretion, one or more subordinate CAs can be established under this CP with the subordinate CA's root certificate being signed by the highest level CA. Subordinate CAs may have a CPS that differs from the root CPS but it must still align with the CP.

1.1.3 CROSS CERTIFICATION

Cross Certification of CRA Internal CA with other GC CAs will be achieved through the Canadian Federal PKI Bridge (CFPB) where policy mapping will be done.

CRA External CA is not cross-certified with other GC CAs.

1.2 NAME AND IDENTIFICATION

This document is identified by object identifier: 2.16.124.101.1.272.3.#.1.1.1

{joint-iso-itu-t(2) country(16) ca(124) gc(101) gcOrg(1) cra (272) certpcy(3) documents(#), PersonUser(1), Version(1), SubVersion(1)}

All certificates issues under this policy will contain this Object Identifier in the X509v3 Certificate Policies field.

Certificates issued in accordance with this Certificate Policy will assert one of the Object Identifiers (OIDs) in the certificate policy extension. Note: Level 0 should only be used in testing environments.

TABLE 1: CRA PKI CERTIFICATE TYPE NAMES AND CORRESPONDING OIDS

id-cra-certpcy-Level_0-PersonUser	2.16.124.101.1.272.3.#.1.0
id-cra-certpcy-Level_1-PersonUser	2.16.124.101.1.272.3.#.1.1
id-cra-certpcy-Level_2-PersonUser	2.16.124.101.1.272.3.#.1.2
id-cra-certpcy-Level_3-PersonUser	2.16.124.101.1.272.3.#.1.3

{joint-iso-itu-t(2) country(16) ca(124) gc(101) gcOrg(1) cra (272) certpcy(3) Certificates (#) PersonUser(1) Certificate(#)}

1.3 PKI PARTICIPANTS

The section identifies the roles relevant to the administration and operation of CAs under this policy.

1.3.1 CERTIFICATION AUTHORITIES

1.3.1.1 CANADA REVENUE AGENCY CERTIFICATE POLICY AUTHORITY

This policy is issued under the authority of Canada Revenue Agency (CRA).

1.3.1.2 MANAGEMENT AUTHORITY

The CRA PKI Management Authority is the organization that operates and maintains the Certificate Authority (CA) on behalf of the Certificate Policy Authority (CPA).

It is the Management Authority’s responsibility to develop a Certificate Practice Statement (CPS) that conforms with this Certificate Policy.

1.3.1.3 CRA PKI MANAGEMENT AUTHORITY

The CRA PKI Policy Management Authority (CRA PKI PMA) is the CRA management body responsible for governance of all use of PKI, certificates, and cryptography within CRA and CBSA.

The CRA PKI PMA is responsible for:

1. Appointing the CRA CA;
2. Approving this CP and the associated Certification Practice Statement;
3. Approving the establishment, maintenance and termination of cross-certification or other interoperability agreements with other GoC PKI CAs; and
4. Approving requests for cross-certification or for other interoperability agreements with CAs, whether members of the GoC PKI or external to the GoC PKI.

1.3.2 REGISTRATION AUTHORITIES

1.3.2.1 REGISTRATION AUTHORITY

The Registration Authority (RA) collects and verifies each subscriber identity and information that is to be entered into the subscriber’s public key certificate. The RA performs its functions in accordance with a CPS approved by the Certification Authority. The RA is responsible for:

a) The registration process;
b) The identification and authentication process;
c) Initiating or relaying change requests for certificates (i.e. *RFC822*);
d) Initiating or relaying revocation requests for certificates and
e) Approving applications for renewal or re-keying certificates on behalf of a Certification Authority.

The functions which the RA may carry out will vary from case to case but may include personal authentication, token distribution, revocation reporting, name assignment, key generation, deactivations and archival of key pairs.

When the RA is not present, the CA is assumed to be able to carry out the RA’s functions so that PKI management protocols are the same from the Subscriber’s point of view.

An RA is itself a Subscriber and may also perform its role utilizing an electronic (online) authentication method.

1.3.2.2 LOCAL REGISTRATION AUTHORITY

A Local Registration Authority (LRA) is a trusted agent for a specific constituency, with the authority for identity verification and approving the application request remote from the CA.

The RA verifies the authority of the LRA to act on behalf of a specific constituency. The validation of the authority of these individuals is described in section 3.2.5.

1.3.3 SUBSCRIBERS

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. Subscribers include CRA and CBSA employees. CAs are sometimes technically considered “subscribers” in a PKI. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

Those external to the CRA and CBSA must agree to abide by the terms and conditions of an Organization Agreement: Appendix C Subscriber Agreement prior to being issued public key certificates signed by the CA operating under this Certificate Policy.

Only under exceptional circumstances and with the authorization of the CA, may an individual act on behalf of another individual other than themselves (e.g. disability, etc.) if their identity can be authenticated to satisfy the terms and conditions of this CP. In such cases, operational safeguards must be put in place to ensure the binding of key usage to the individual is maintained.

1.3.4 RELYING PARTIES

A Relying Party is a recipient of a certificate who relies on the validity of the binding of the Subscriber's name to a public key.

A Relying Party is either:

a) A Subscriber of the CRA PKI; or
b) An individual or organization external to CRA and CBSA who has received a digital certificate from a CA, which has signed a cross-certification agreement with the GC PKI or has entered into another kind of arrangement acceptable to the TBS, CIOB

1.3.5 OTHER PARTICIPANTS

This CA and its associated RAs may require the services of other security, community, or application authorities. The Certification Practice Statement (CPS) will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.5.1 NON-CRA/CBSA ENTITIES

A non-CRA/CBSA entity is an organization external to the CRA and CBSA that assumes all responsibility for the identification and authentication activities performed and all use of certificates issued under their direction.

The Commissioner of Canada Revenue Agency may, in its sole discretion, determine whether an organization may be part of the CRA PKI.

1.3.5.2 REPOSITORY MANAGER

The Repository Manager is an individual or organization responsible for maintaining one or more:

a) Repositories holding relevant information such as certificates and Certificate Revocation Lists; or
b) On-line Certificate Status Protocol servers.

Where certificates identify the CRL as an authoritative source for revocation information, the operations of that authority are within the scope of this CP. An Online Certificate Status Protocol Server shall assert all the policy OIDs for which it is authoritative. This policy does not cover OCSP servers that are locally trusted.

1.3.5.3 APPLICATION RESPONSIBLE OWNER

An Application Responsible Owner (ARO) is an individual within the CRA or CBSA who is responsible for the management of a particular application (e.g., departmental e-mail system), or program (e.g., security).

The ARO is responsible for any Program-specific enrolment requirements and may impose further requirements over and above those specified by this certificate policy.

The ARO, supported by Agency Security Officers, shall determine the appropriate certificate policies for their applications in accordance with this policy.

1.3.5.4 PKI SERVER OPERATOR

The PKI server operator is responsible for the configuration and maintenance of hardware and software for the CA system, for the commencement and cessation of CA services and for the initial creation of accounts for PKI Security Officers.

1.3.5.5 PKI SECURITY OFFICER

The PKI Security Officer is responsible for the management of PKI Administrators as well as other PKI Security Officers and the configuration of CA security policy.

1.3.5.6 PKI ADMINISTRATOR

The PKI Administrator is responsible for the management of the Subscriber initialization process; the creation, renewal or revocation of certificates; and the distribution of tokens (where applicable). The PKI Administrator can also fulfill the role of a Registration Authority.

1.3.5.7 ONLINE REGISTRATION AND CREDENTIAL ADMINISTRATION

Only for Level of Assurance (LOA) Level 1-2, an online registration and authentication service can be used for the issuance of an ID-based PKI certificates. This service enables employees of CRA and CBSA to securely create and manage their PKI identity-based credentials.

1.4 CERTIFICATE USAGE

This CPs identifies three discrete types of certificates aligned with the *Standard on Identity and Credential Assurance* (Reference C) and the *Guideline on Defining Authentication Requirements* (Reference D). These are the same levels as internationally standardized in the International Standard detailing the "*Entity authentication assurance framework*" (Reference H).

All subscriber certificates issued under this CP are intended for the exclusive use of the person to who the certificate was issued.

A subscriber certificate type may be implemented using two certificates where Digital Signature certificates are separated from Confidentiality (encryption) certificates. Under no circumstances will a signing certificate be used for encryption or vice versa. For more information on key usage see paragraph 6.1.7.

Each CA asserting this policy must state the acceptable and prohibited usage requirements in the CPS and inform Subscribers of their usage limitations.

The level of Identity Proofing is as detailed in the *Standard on Identity and Credential Management* (Reference C) and the *Guideline on Defining Authentication Requirements* (Reference D).

The level of Credential type is as detailed in the *User Authentication Guidance for Information Technology Systems* (Reference I).

Table 2: Certificate usage

Effective Level of Assurance	Level of Identity Proofing	Level of Credential Type	Usage
Level 3	Level 3	Level 4 – Hardware based credential	Digital Signature, nonrepudiation, key Encipherment, key Agreement
Level 2	Level 2	Level 2 - Software based (can be exportable) credential	Digital Signature, nonrepudiation, key Encipherment, key Agreement
Level 1	Level 1 used for pseudo-anonymous users	Level 2 - Software based (can be exportable) credential	Digital Signature, nonrepudiation, key Encipherment, key Agreement
Level 0	Level 0 is for testing	Level 0 – This can be hardware or software. There is no assurance associated with this type of certificate.	Digital Signature, nonrepudiation, key Encipherment, key Agreement

1.4.1 APPROPRIATE CERTIFICATE USES

Subject to any legislative or regulatory requirements applicable to a program and to a threat and risk assessment of an application, certificates may be used in applications for CRA/CBSA purposes:

a) Digital signature services (authentication and data integrity);
b) Protection (confidentiality);
c) Technical (non-repudiation);

Certificates may also be used to satisfy other general or specific requirements of the CRA or CBSA, upon approval by the CRA PKI PMA.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates issued by the CA shall not be used for:

a) Transactions where applicable law prohibits the use of digital signatures for such transactions or where otherwise prohibited by law;
b) The protection of Protected C or Classified information, unless supported by other appropriate security mechanisms and procedural safeguards.

Subscribers shall not use CRA PKI certificates to facilitate and/or conceal an unauthorized act as specified in Federal law or Government of Canada acts, legislation and/or regulations. Examples of such actions include, but are not limited to, the following:

a) Use of PKI certificates to gain unauthorized access to a CRA or CBSA facility, information system, or electronic data (e.g. Privacy information), or to enable others to gain such access;
b) Transferring information to an unauthorized individual; or
c) Generating income for oneself or for an organization.

1.5 CERTIFICATE POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The CRA PKI Policy Management Authority (CRA PKI PMA) is responsible for all aspects of this CP.

1.5.2 CONTACT INFORMATION

PKI Management Centre
Canada Revenue Agency
1st Floor, 20 Fitzgerald
Ottawa, Ontario, K1A 0L5
Canada

PKIADMINICP@cra-arc.gc.ca

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The CRA PKI PMA, shall approve the CPS for each CA that issues certificates under this policy.

1.5.4 CPS APPROVAL PROCEDURES

CRA PKI PMA shall approve the CPS associated with this Certificate Policy and any amendments thereto, following a determination that the CPS sets out in a satisfactory manner how the CA will implement the requirements of this Certificate Policy.

1.6 DEFINITIONS AND ACRONYMS

TABLE 3: GENERAL DEFINITIONS

Term	Definition
Authorization Authority	A Management Entity with the authority to permit a PKI Entity to operate within a particular domain and acceptance by that Management Entity of the associated residual risk. The CIO of the Government of Canada is responsible for the authorization of the common CAs as defined by the "*Guideline on the Management of Public Key Infrastructure in the Government of Canada*" (Reference K).
Activation data	Private data, other than keys, required to access Personal Security Environments that needs to be protected (e.g., password).
Application Responsible Owner	An individual within a department or agency who is responsible for the management of a particular application (e.g., departmental e-mail), program (e.g., security), particular program or horizontal activity which spans multiple departments or agencies.

Term	Definition
Authority Revocation List	A list of revoked CA certificates. An ARL is a Certificate Revocation List for CA cross-certificates or self-signed certificates.
Canadian Federal PKI Bridge	Under the direction of the GC PKI Policy Management Authority, the CFPB signs and manages cross-certificates with GC top-level CAs as well as with non-GC CAs.
Certificate	An electronic file in a format which is in accordance with ITU-T Recommendation X.509 and which contains a public key of a Subscriber together with related information, digitally signed with the private key of the Certification Authority that issued it.
Certificate Revocation List	A list issued and maintained by the Certification Authority of the certificates that are revoked before their pre-set expiry time.
Certificate Status Authority	An Entity trusted to provide on-line verification to a Relying Party of a certificate’s validity and which may also provide additional attribute information for the certificate.
Certificate Policy Authority	The organization which approves the Certificate Policy and all Certificate Practice Statements.
Certificate Authority	Also referred to as a Certification Authority, a Certificate Authority is an Entity, trusted by one or more End Entities, which issues and manages X.509 public key certificates and CRLs. Each CA within the CRA PKI may issue certificates under a choice of policies based on the level of assurance to which the CA has been accredited.
Certification Authority Software	Software that manages the CA signing key, the life cycle of certificates and CRLs as well as key pairs of End Entities.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in issuing certificates. The CPS must either contain, or point to other sources which contain, sufficient information to demonstrate to the applicable authority how the requirements contained within the CP or CPs are being met.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.

Term	Definition
Certification Validation Chain	A chain of certificates beginning with the certificate of a public key holder (an Entity) signed by one CA – the certificate of the CA of the Entity - and one or more additional certificates of CAs signed by other CAs. If the public-key user (Relying Party) does not already hold an assured copy of the public key of the CA that signed the Entity's certificate, the CA's name, and related information (such as the validity period or name constraints), then it may need an additional certificate to obtain that public key for verification purposes. Often, a chain of multiple certificates may be needed. Such chains are called certification paths.
Configuration Management	A process to identify and define critical items in the system and to control any change of these items throughout their lifecycle.
Cross-certificate	A certificate issued by a Certification Authority to establish a trust relationship between it and another Certification Authority.
Custodian	An individual making a certificate request on behalf of a device or application and responsible for certificate management activities requiring human interaction. Upon acceptance of the certificate issued, the obligations of the subscriber extend to the custodian of the certificate.
Data Integrity	When digital signatures are used, the assurance that the data is unchanged from the moment that a digital signature is applied to the data. There are other means to achieve data integrity, such as the use of Message Authentication Codes.
Designated Organization	An organization that is authorized to appoint an LRA for registration of individuals, devices, applications, or roles within that organization assuming all responsibility for the identification and authentication activities performed and all use of certificates issued under their direction.
Designated Responsible Individual	An individual within a Designated Organization authorized by it to represent and to act on behalf of the organization for the purpose of applying for the issuance of certificates.
Digital Signature	The result of a transformation of data by means of a cryptographic system using keys such that a person who receives the initial data can determine whether: • The transformation was created using the key that corresponds to the signer's key; and • The data has been altered since the transformation was made.

Term	Definition
End-Entity	An Entity that uses the keys and certificates created within a Public Key Infrastructure for purposes other than the management of keys and certificates. An End-Entity may be a Subscriber, a Relying Party, or a device, a role or an application using a certificate assigned to them.
Enrolment	A process by which an individual can register to receive services from, or make transactions with, a Specific Program.
Enterprise Certificate	A certificate issued by a CA for use by individuals, roles or groups, devices or applications. These certificates are fully managed within a PKI and may be subject to: • Automatic revocation checking; • Transparent credential update; and • Dynamic and transparent security policy update. An Enterprise certificate securely binds the owner of the certificate to its public keys. Enterprise Certificates use separate keys for digital signature and for confidentiality.
Entity	An autonomous element within the PKI. This may be a CA, a trusted role within a CA, an RA or an End-Entity.
Group Custodian	An individual representing a group for which a certificate has been issued and responsible for certificate management activities requiring human interaction. Upon acceptance of the certificate issued to the group, the obligations of the subscriber extend to anyone using the certificate. Group certificates do not have digital signature or non-repudiation assurance.
Individual	A single, natural person as distinguished from a group or class of individuals or any type of organization.
Initialization data	Codes or other data used by a Subscriber to generate a private digital signature key and obtain public key certificates from the CA (e.g. reference number and authentication code).
Local Registration Authority	The certificate registration function of identity verification and application approval performed local to a specific constituency. Within a client organization, the Designated Responsible Individual (DRI) is authorized to perform the LRA duties within the client organization or department respectively.

Term	Definition
Network Security Zone	A Network Security Zone, as defined in *ITSG-22 Baseline Security Requirements for Network Security Zones (Reference L)*, demarcates a logical area within a networking environment with a defined level of network security.
Non-repudiation	In a legal context, non-repudiation means sufficient evidence to persuade an adjudicator as to the origin and data integrity of digitally signed data, despite an attempted denial by the purported sender. In a technical context, non-repudiation refers to the assurance a Relying Party has that if a public verification key is used to validate a digital signature, that signature had to have been made by the corresponding private signing key.
Object Identifier	The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
Operations Zone	An Operations Zone (OZ), as defined in *ITSG-22 Baseline Security Requirements for Network Security Zones (Reference L)*, is the standard environment for routine GC operations. It is the environment in which most end-user systems and workgroup servers are installed.
Organization	A government other than GC or an agency, corporation, partnership, trust, joint venture or other association. If recognized as such, an organization may include a sole proprietorship.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of managing certificates and keys.
PKI Administrator	An individual responsible for the: a) Management of the Subscriber initialization process; b) Creation, renewal or revocation of certificates; and c) Distribution of tokens (where applicable).
PKI Admin User	An individual responsible for the: a) Configuration and maintenance of hardware and software for the CA system; b) Commencement and cessation of CA services; and c) Initial creation of accounts for PKI Security Officers.
PKI Security Officer	An individual who is responsible for the management of PKI Administrators as well as other PKI Security Officers and the configuration of CA security policies.
Program	A specific set of government services to be offered through electronic means.

Term	Definition
Program Business Manager	An individual within a Department or agency who is responsible for management of a particular Government of Canada Program.
Public Zone	A Public Zone, as defined in *ITSG-22 Baseline Security Requirements for Network Security Zones (Reference L)*, is entirely open and includes public networks such as the public Internet and the public switched telephone network (PSTN).
Public Access Zone	A Public Access Zone (PAZ), as defined in *ITSG-22 Baseline Security Requirements for Network Security Zones (Reference L)*, mediates access between operational GC systems and the Public Zone. The interfaces to all Government On-Line services should be implemented in a PAZ.
Registration Authority	A person that is responsible for the identification and authentication of Subscribers and other End Entities, but does not sign or issue the certificates. An RA may be asked to perform certain tasks by the CA.
Re-key	Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.
Repository	A system where CRLs, ARLs and public key certificates are stored for access by Entities. An X.500 directory is an example of a repository.
Repository Manager	An individual or role responsible for maintaining one or more: a) Repositories holding relevant information such as certificates and Certificate Revocation Lists; or b) On-line certificate status checking servers.
Restricted Zone	A Restricted Zone, as defined in *ITSG-22 Baseline Security Requirements for Network Security Zones (Reference L)*, provides a controlled network environment suitable for business-critical IT services.
Role Holder	An individual representing a role for which a certificate has been issued and responsible for certificate management activities requiring human interaction. Upon acceptance of the certificate issued to the role, the obligations of the subscriber extend to the role holder.
Secure Container	Any totally enclosed storage space for a classified asset, as specified in *Operational Security Standard on Physical Security* (Reference M).

Term	Definition
Storage	A process during which private signature keys and private confidentiality keys are stored in a profile located on a server operated by the CA. When Subscribers wish to use their keys, they access their profile using a specific user ID and password known only to them; retrieve the encrypted profile using a secure protocol and, following its use, the local copy of the profile is destroyed. A Subscriber may also store their profile locally. At no time is the profile outside the exclusive control of the Subscriber.
Subordinate Certificate Authority	A Certificate Authority where the CA's root certificate operates under the authority (signature) of another (superior) CA. Normally, the Subordinate CA will use the same CP as the higher level (superior) CA but may have a different CPS.
Subscriber	An entity enrolling with a CA for a certificate through a registration and approval process. Prior to certificate issuance, the subscriber must either sign a contract which contains the provisions of a subscriber agreement within it or a subscriber agreement itself, or otherwise agree to abide by the terms of a Subscriber Agreement. Within the GC, employees are bound to abide by the terms of Acceptable Use Policy.
Web Certificate	A certificate issued to users (e.g. clients and servers) by a CA, securely binding the owner of the certificate to its public keys. A root key for the CA is typically embedded within commercial browsers thus enabling verification of these Web certificates. Web certificates use a single key pair and certificate for both digital signature and confidentiality. Web certificates are outside the scope of this CP.

TABLE 4: ACRONYMS

TERM	DEFINITION
ARL	Authority Revocation List
ARO	Application Responsible Owner
CA	Certificate Authority
CFPB	Canadian Federal PKI Bridge
CIO	Chief Information Officer

TERM	DEFINITION
CIOB	Chief Information Officer Branch
CP	Certificate Policy
CPA	Certificate Policy Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CSS	Certificate Status Server
DN	Distinguished Name
DRI	Designated Responsible Individual
DSA	Digital Signal Algorithm
ERC	Enhanced Reliability Check
FIPS	Federal Information Processing Standards
GC	Government of Canada
GOL	Government of Canada On-Line
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PBM	Program Business Manager
PGS	Policy on Government Security
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure

TERM	DEFINITION
PKIX	The Working Group from IETF responsible for developing Internet standards to support X.509-based Public Key Infrastructures (PKIs)
PSE	Personal Security Environment
RA	Registration Authority
RDN	Relative Distinguished Name, as per the X.509 standard.
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman
SA&A	Security Assessment and Authorization
SHA	Secure Hash Algorithm
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
URL	Uniform Resource Locator

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The CA will have at least one certificate and CRL repository associated with it. The CA may, but need not, perform this function itself.

Where a repository is not under the control of the CA, the CA shall establish terms and conditions of its association with the Repository Manager which shall include, but are not limited to, the subjects of availability, access control, integrity of data, protection of personal information, directory replication, directory chaining, and if applicable, directory referrals.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

Where the CA operates a repository or otherwise acts as a repository manager, the CA shall:

a) Publish certificates and CRLs;
b) Inform Subscribers of the location of any CRL or OCSP server; and
c) Publish the status of certificates through certificate revocation lists, OCSP servers, or otherwise make information available within the timeframes specified in this Certificate Policy.

2.2.2 PUBLICATION OF CA INFORMATION

With regard to policy and practices, the CA shall:

a) Publish this Certificate Policy at:

Internal site: http://infozone/english/r2423153/dtim_gidt/sc/pki_icp/index/index-e.asp

External site: https://www.canada.ca/en/revenue-agency/services/e-services/public-key-infrastructure/about-public-key-infrastructure.html

b) Publish public key certificates and current certificate status information using CRLs and optionally OSCP servers; and
c) Publish, or cause Departments/Organizations to publish, Subscribers and Relying Parties rights, obligations, entitlements or permissions, and any changes concerning their rights, obligations, entitlements or permissions with respect to certificates.

2.3 TIME OR FREQUENCY OF PUBLICATION

An updated version of the CP will be made publicly available within 30 calendar days of approval.

2.4 ACCESS CONTROLS ON REPOSITORIES

The CA shall protect any repository information not intended for public dissemination or modification.

The CA shall configure operating system and repository access controls so that only authorized CA personnel can write or modify the on-line version of the CP. Direct and/or remote access to other information in the CA repositories shall be determined by the CA.

The appropriate CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

The Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile *https://tools.ietf.org/html/rfc5280* document should be referenced when determining the content of certificates.
CAs external to the GC must ensure their naming and identification of Subscribers are PKIX compliant.

3.1 NAMING

3.1.1 TYPES OF NAMES

The Distinguished Name (DN) field in the certificate must be a Distinguished Name attribute type as defined in X.520 (Reference F) and implemented as per X.509 (Reference G).

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the certificate holder to which they are assigned. When DNs are used, it is preferable that the common name represents the certificate holder in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and/or serial number, or an application process. The CA shall use DNs in certificates it issues. When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3 for LOA 0 & 1 certificates.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Subscriber certificates shall not contain anonymous or pseudonymous identities.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The rules for interpreting name forms are specified in X.501 (Reference E).

The fact that a name is spelled without its accented characters does not preclude its conformity to the official name.

3.1.5 UNIQUENESS OF NAMES

Distinguished names must be unique for all end entities. X.500 distinguished names shall be used, and the CA and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Where permitted or required, the use of a trademark is reserved to the holder of that trademark.

3.2 INITIAL IDENTITY VALIDATION

The CA or RA shall ensure that a record is kept of:

a) the name of the individual;
b) the attestation made by the LRA to the fact that the identification and authentication was done;
c) the means by which the identity of the role holder or custodian has been established and authenticated.

> Practice Note: The requirement for initial identification will vary amongst the assurance levels. The Standard on Identity and Credential Assurance (Reference C) and the Guideline on Defining Authentication Requirements (Reference D) should be used in developing the practice statements. Additionally, the US "Electronic Authentication Guideline" (Reference J) can be used as a guideline, chapter 5.3 of this document is recommended for review when developing the practice statement(s).

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

Prior to the issuance of a verification certificate, the CA and Subscriber will confirm their possession of the corresponding private key in a manner consistent with IETF standard as that described in section 4.3 of RFC 4210 (CMP), or RFC 5272 (CMC).

3.2.2 AUTHENTICATION OF AN ORGANIZATION IDENTITY

3.2.2.1 LEVELS 1 AND 2 ASSURANCE

Employees and agents of an organization must make an application to be a Subscriber through an individual having authority to act on behalf of the organization.

The identity of an organization must be authenticated in any manner sufficient to satisfy the CA that the organization has the identity it claims to possess. The authentication of the identity of the organization may be done by using any of the following means:

a) Privately shared information if the identity of the organization has been previously established by a Program for enrolment purposes; or
b) Copies of official documentation providing evidence of the existence of the organization.

The CA or RA must also verify the identity and authority of the individual acting on behalf of the organization and that individual's authority to receive the keys on behalf of that organization.

The CA or RA shall ensure that a record is kept of the means by which the identity of the organization and the individual authorized to act on behalf of the organization has been established, and of any type of identification used, but is not obliged to keep a copy of the identification itself.

3.2.2.2 LEVEL 3 ASSURANCE

In addition to the identification and authentication above, the individual with the authority to act on behalf of the organization must personally present him or herself to the CA or RA prior to token initialization.

3.2.3 AUTHENTICATION OF AN INDIVIDUAL IDENTITY (IDENTITY PROOFING)

3.2.3.1 LEVEL 1 ASSURANCE

No requirement for identity proofing is required for level 1 assurance.

3.2.3.2 LEVEL 2 ASSURANCE

An application to become a subscriber must be submitted by an authorized person representing an approved organization.

The identity of a prospective Subscriber must be authenticated to satisfy the CA or RA that the individual has the identity he or she claims to possess. Prior to submitting the request to the CA, the LRA shall authenticate the identity of a prospective Subscriber using any of the following means:

a) Privately shared information if the identity of the individual has been previously established;
b) Two pieces of identification (notarized copies or originals), one of which must be government-issued identification containing verifiable biometric information such as a photograph or finger print, and one of which must contain a signature. For CRA or CBSA employees one piece of ID must be the CRA or CBSA issued employee card;
c) A digital signature using a certificate issued by another CA recognized by the TBS, CIOB or cross-certified with the CFPB provided that the Assurance Level of the signing certificate used is not lower than the Assurance Level of the certificate being requested.

Departments and Agencies may also require other information, proofs of credentials or authorization for enrolment in a Program.

The CA or RA shall ensure that a record is kept of the means by which the identity of the individual has been established, and of any type of identification used.

3.2.3.3 LEVEL 3 ASSURANCE

In addition to the identification and authentication, that prospective Subscriber must personally present him or herself to the CA or RA, or to a Designated Responsible Individual that has personally presented him or herself to the CA or RA prior to vouching for that individual, prior to token initialization.

Practice note: The practice statement will detail procedures required to meet this policy. The procedures should have different procedures dealing with employees and contractors. In the case of employees, it is acceptable to verify identity using internal government databases (example: a secure database with the person’s photo). For contractors, if a building pass was issued and identity proofing done then this can be used as a basis to meet the identity proofing requirement.

3.2.3.4 INDIVIDUAL ON BEHALF OF ANOTHER INDIVIDUAL FOR LOA LEVEL 1 – 2 ONLY

Under exceptional circumstances (e.g. disability, language barrier) as authorized by the CA, an individual may seek to be a Subscriber through a request submitted by another individual authorized to act on their behalf.

Prior to submitting the request to the CA, the LRA shall authenticate the identity of both the requestor and the prospective Subscriber, in the same manner that it authenticates an individual on his or her own behalf.

The permission granted by one individual to another, to act on his or her behalf, must be attested. The circumstance necessitating this permission must be authorized by the CA.

The LRA must provide the following information to the CA:

a) Identification of the requestor and the prospective Subscriber;
b) Attestation to the fact that the identification and authentication was done;
c) Attestation that permission was granted authorizing one individual to act on behalf of another, and that CA authorization was obtained; and
d) Contact information to enable the CA or RA to communicate with the individuals and the LRA.

The CA or RA shall ensure that a record is kept of the information provided by the LRA to the CA and the means by which the identity was established and authenticated, but is not obliged to keep a copy of the identification itself.

The CA or RA shall ensure that a record is kept of the information provided by the LRA to the CA identifying the exceptional circumstance, and authenticating the permission for one individual to act on behalf of another. A record of the CA authorization is kept.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Level 1 certificates by design have non-verified subscriber information.

3.2.5 VALIDATION OF AUTHORITY

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate their individual’s authority to act in the name of the organization.

The CA or RA shall ensure that a record is kept of the means by which the identity of the individual has been established and authenticated, and of any type of identification used, but is not obliged to keep a copy of the identification itself.

3.2.6 CRITERIA FOR INTEROPERATION

The CA is governed by the *Guideline on the Management of PKI Infrastructure in the Government of Canada* (Reference K) for agreements for cross-certification and the recognition of other CAs.

3.3 3.3 IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

A request for re-key may be presented by the Entity in whose name the keys have been issued. All requests for re-key must be authenticated by the CA, and the subsequent response must be authenticated by the Entity.

An Entity requesting re-key may authenticate the request using its valid Digital Signature key pair.

Where one of the keys has expired, the request for re-key must be authenticated in the same manner as initial registration.

Requests for routine re-keys must be recorded in a log.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Where the information contained in a certificate has changed or there is a known or suspected compromise of a private key, the CA must authenticate a re-key in the same manner as for initial registration.

Any change in the information contained in a certificate must be verified by the CA or an RA authorized to act on behalf of that CA before that certificate is issued, except where the CA has determined that multiple changes to the DNs of Subscribers or Designated Certificate Holders is the result of organizational changes within a Client Organization.

Requests for re-key after revocation of certificates must be recorded in a log.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The CA or RA must authenticate a request for revocation of a certificate. The authentication may be performed using privately shared information.

A Subscriber requesting revocation may authenticate the request using its private signing key, regardless of whether or not the private signing key has been compromised.

The CA must ensure revocation requests are authenticated and confirm that the person making the revocation request is the subscriber or the request is done by the authorized representative of the subscriber with authority to make the revocation request as further described in the CPS.

Upon receipt of a Request for Revocation for possible compromise, the CA will revoke the certificate. This is to make sure that the certificate cannot be recovered through an on-line recovery system.

Requests for revocation of certificates must be recorded in a log.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The Certificate application process must provide sufficient information to:

a) Establish the applicant’s authorization (by the employing or sponsoring agency) to obtain a certificate (per section 3.2.3);
b) Establish and record identity of the applicant (per section 3.2.3);
c) Obtain the applicant’s public key and verify the applicant’s possession of the private key for each certificate required (per section 3.2.1); and
d) Verify any role or authorization information requested for inclusion in the certificate.

Online Requests may be available through a web link where applicants can self-perform PKI key creations and recoveries for LOA level 1 and Level 2.

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

The types of applicants permitted as Subscribers of the GC are described in section 1.3.3.

Bulk applications for certificates are permitted but may only be made by persons authorized to make such applications such as an ARO or through an LRA.

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

Individuals wishing to obtain Level 2, 3 or 4 certificates must obtain authentication and approval from either an RA or LRA. RA or LRA responsibilities in processing the various types of applications are described in section 1.3 (PKI Participants) and section 3.2 (Initial Identity Validation).

A request for a certificate is separate and distinct from any Departmental or Agency process for enrolment in, or the use of, a Program. An ARO may impose additional requirements and require additional information, proof of credentials or authorization for the purpose of granting access to a Program. In certain circumstances, other authorizations may be required, which will be elaborated in the CPS.

4.1.2.1 LEVEL 0 ENROLMENT AND RESPONSIBILITIES

No stipulation

4.1.2.2 LEVEL 1 ENROLMENT PROCESS AND RESPONSIBILITIES

As the Level 1 certificate type is designed for pseudonymous use, there is no stipulation as to the enrolment process; however, the CPS will provide more detail as to how enrolment is achieved.

4.2 CERTIFICATE APPLICATION PROCESSING

For the issuance of Certificates, the CA shall state in the CPS:

a) All procedures and requirements with respect to applications for the issuance of certificates; and
b) The information that prospective Subscribers must submit and the application process.

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The CA must ensure that each application is accompanied by:

a) Proof or confirmation of the Subscriber’s identity as per sections 3.2.2 and 3.2.3; and
b) When requested by the CA, proof or confirmation of authorization for any requested certificate and or certificates attributes.

Additionally, for applications approved, the RA or LRA must confirm that an agreement exists with the CA for registration from the specific local constituency:

> DRIs shall refer to the name of the Designated Organization, the date of execution of the agreement or any contract identifier to indicate the agreement their organization signed concerning its rights, privileges and obligations associated with certificates issued, or to be issued, on behalf of the Designated Organization.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The issuance of a certificate by the CA occurs only upon complete and final approval of the certificate application by the CA.

An application for a certificate does not oblige the CA to issue a certificate. The CA has the discretion to reject a request for a certificate.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

There is no stipulation for the period between the receipt of an application for a certificate and the generation of the Entity's key material.

4.2.3.1 LEVEL 2 ASSURANCE

The CA must ensure that the Entity has to complete its initialization process no longer than 14 calendar days after creation of the activation data.

4.2.3.2 LEVEL 3 ASSURANCE

The CA must ensure that the Entity has to complete its initialization process within 24 hours upon receipt of activation data.

4.3 CERTIFICATE ISSUANCE

The publication of a certificate by the CA in the repository indicates a complete and final approval of the certificate application by the CA.

The issuance of a certificate by the CA is separate and distinct from any Departmental or Agency process for enrolment in a Program.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

The certificate is published in the repository. Upon issuance, the certificate will be assigned to the individual.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

Except as otherwise stipulated, publication of a certificate in a repository constitutes the CA's certification, and notice to a Subscriber or a Relying Party who may access the certificate in the repository, that the information stated in the certificate was verified in accordance with this Certificate Policy for the assurance level for which it was issued.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The use of the certificate by the individual for which a certificate has been issued constitutes acceptance of a certificate and all obligations associated with its use.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

As specified in Section 2.2.1, each GC CA shall publish all appropriate CA and Subscriber certificates in the appropriate certificate repositories.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Except as otherwise stipulated, publication of a certificate in a repository constitutes the CA's certification and notice to a Relying Party who may access the certificate in the repository, that the information stated in the certificate was verified in accordance with this Certificate Policy.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers and CAs shall protect their private keys from access by any other party.

Subscribers and CAs shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:
a) The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CP.
b) That the certificate is being used in accordance with its Key-Usage field extensions; and
c) That the certificate is valid at the time of reliance by reference to OCSP or CRLs.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised and the subscriber name and attributes are unchanged.

4.6.2 WHO MAY REQUEST RENEWAL

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The CRA CA does not support certificate renewal.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

As specified in Section 2.1, each GC CA shall publish all appropriate CA and Subscriber certificates in the appropriate certificate repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Re-key of a certificate does not require a change to the *subjectName* and does not violate the requirement for name uniqueness.

The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

The CA shall retain Subscriber decryption key history as a result of Certificate Re-Key. The storage of keys by the CA shall be used strictly for authorized key recovery and business continuity purposes.

The retention period will be as stated in the CPS.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

A certificate re-key may be performed for any of the following reasons:

a) expiration of a certificate;
b) loss or compromise of the certificate;
c) issuance of a new hardware token; or
d) when the certificate is revoked and a new certificate is authorized (i.e., the Subscriber is still a valid Subscriber).

A certificate shall not be eligible for automatic re-key while in revoked or suspended status.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

A request for re-key may be presented by the Entity in whose name the keys have been issued or by another individual authorized to act on behalf of the Entity. All requests for re-key must be authenticated by the CA, and the subsequent response must be authenticated by the Entity or by another individual authorized to act on behalf of the Entity.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Where one of the keys has expired, the request for re-key must be authenticated in the same manner as initial registration.

An Entity requesting re-key may authenticate the request using its valid Digital Signature key pair.

Requests for routine re-keys must be recorded in a log.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As per section 4.3.2(Notification to Subscriber by the CA of Issuance of Certificate)

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As per section 4.4.1(Conduct Constituting Certificate Acceptance).

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As per section 4.4.2(Publication of the Certificate by the CA).

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As per section 4.4.3(Notification of Certificate Issuance by the CA to other Entities).

4.8 CERTIFICATE MODIFICATION

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

No stipulation.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

No stipulation.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

No stipulation.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF A MODIFIED CERTIFICATE

No stipulation.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

No stipulation.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.9 CERTIFICATE REVOCATION

4.9.1 CIRCUMSTANCES FOR REVOCATION

Upon receipt of acceptable notification, the CA shall revoke/suspend a certificate in the following circumstances:

a) Upon the suspected or known compromise of the private key or the media holding the private key;
b) Upon the death or cessation of employment of a Subscriber;
c) Upon the termination of the requirement of a group; or
d) Upon a properly authenticated request by a Subscriber to revoke their certificates.

The CA, in its discretion, may revoke a certificate when a Subscriber fails to comply with any agreement, any applicable law, where the Subscriber has not used his or her private keys over the previous 18 months, or where the CA reasonably believes it appropriate in the circumstance.

4.9.2 WHO CAN REQUEST REVOCATION

The revocation or suspension of a certificate may only be requested by:

a) A Subscriber;
b) An individual authorized to act on behalf of the Subscriber as specified in section 3.2.3.4;
c) An LRA assigned with responsibility for administering requests for the Subscriber to be revoked;
d) Authorized CA personnel at their own discretion or on the request of a Subscriber, LRA or custodian;
e) An automated process acting on behalf of the CA.

The revocation of a cross-certificate may only be requested by:

a) The CRA PKI PMA;
b) Authorized Bridge CA personnel (CFPB custodians) under emergency circumstances; or
c) The CA to which the cross-certificate was issued.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

The CA shall:

a) Authenticate the identity and authority of all revocation requests as per section 0 Identification and Authentication for Revocation Request;
b) Record and retain all information pertaining to such requests, including a statement as to the action taken by the CA;
c) Publish notice of the revocation of a certificate in its CRL or OCSP server;
d) Publish notice of the revocation of a cross-certificate in its ARL or OCSP server.
e) Inform the LRA or Subscriber; and
f) The CA shall notify a Subscriber of any revocation of a certificate assigned to them.

4.9.4 REVOCATION REQUEST GRACE PERIOD

There is no grace period for revocation under this policy.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

4.9.5.1 LEVEL 0

No stipulation.

4.9.5.2 LEVELS 1 AND 2 ASSURANCE

Any action taken as a result of a request for the revocation or suspension of a certificate must be initiated:

a) Immediately, if the request is received during the CA's regular business hours;
b) Immediately upon the start of the next business day if the request is received outside of regular business hours as per the CPS; or
c) No later than 72 hours after receipt if the request is received outside of business hours and the next day is not a business day.

4.9.5.3 LEVEL 3 ASSURANCE

Any action taken as a result of a request for the revocation or suspension of a certificate must be initiated immediately upon receipt and must be reflected in the CRL within 1 hour.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

4.9.6.1 LEVELS 1 AND 2 ASSURANCE

A Relying Party shall:

a) Check the status of all certificates in the certificate validation chain against the current CRLs and ARLs prior to relying on such certificates; and

If the check fails, the certificate should not be trusted.

4.9.6.2 LEVEL 3 ASSURANCE

Level 3 Assurance certificates have the same revocation checking requirements as Levels 1 and 2 Assurance. Additionally, for organizations subject to the PGS (Reference Q), Level 3 Assurance end entities shall not cache any revocation information.

Practice note: Use of revoked certificates could have a damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences of using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

The CA must also ensure that its CRL issuance is synchronized with all relevant repositories to permit a Relying Party to access the most recent CRL.

In the event of actual or suspected key compromise, the CA shall issue an up-to-date CRL immediately upon the revocation of a certificate.

4.9.7.1 LEVEL 0 ASSURANCE

A level 0 certificate is for test purposes only. There is no set CRL update period.

4.9.7.2 LEVELS 1 AND 2 ASSURANCE

The CA shall issue an up-to-date CRL at least every twenty-four (24) hours.

4.9.7.3 LEVEL 3 ASSURANCE

The CA shall issue an up-to-date CRL at least every twenty-four (24) hours.

4.9.8 MAXIMUM LATENCY FOR CRLS (IF APPLICABLE)

CRLs shall be published within 1 hour of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issues CRL for the same scope.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

CAs may support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under this policy.

Where on-line status checking is supported, status information must be updated and available to relying parties within 1 hour of certificate revocation.

Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

A relying Party shall check the status of all applicable certificates prior to relying on such certificates.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA’s approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in sections 4.9.7 and 4.9.8.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

When a CA certificate is revoked an ARL must be issued within 1 hour of notification.

Stipulated in sections 4.9.2 (Who can request Revocation), 4.9.7 (CRL Issuance Frequency) and 4.9.9 (On-line Revocation/Status Checking Availability)

There are no other special requirements.

Practice Note: This means that a secure and operational means needs to be established for authorized parties to make this decision and pass the notification to the PKI operations. Operations needs to have 24/7 capability to issue an ARL.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

The CA may affect the equivalent of a suspension by temporarily revoking a certificate and stipulating the reason code is “on hold”. This temporary revocation of a certificate does not affect the obligations of a Subscriber with respect to the private key associated with the certificate.

4.9.14 WHO CAN REQUEST SUSPENSION

As stipulated in section 4.9.2 (Who Can Request Revocation).

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

The CA shall:

a) Authenticate the identity of all requests for the temporary revocation of certificates;
b) Record and retain all information pertaining to such requests, including a statement as to the action taken by the CA; and
c) Publish notice of any temporary revocation of a certificate in its CRL or OCSP server.

4.9.16 LIMITS ON SUSPENSION PERIOD

The CA may terminate the temporary revocation of a certificate when it determines the reasons for the temporary revocation were unfounded or if it determines that the certificate should be revoked for a reason code other that “on hold”.

4.10 CERTIFICATE STATUS SERVICES

The CA is responsible for promulgating certificate status through CRLs and ARLs or in the OCSP Servers.

4.10.1 OPERATIONAL CHARACTERISTICS

CRL characteristics are stipulated in section 7.2 (CRL Profile). All Subscriber PKI software must correctly process all CRL extensions and should be formatted in the X.509 version 3 certificate format as specified in *Request for Comments (RFC) 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [8].

If OCSP servers are deployed, the CA shall comply with the OCSP characteristics as stipulated in section 7.3(OCSP Profile).

4.10.2 SERVICE AVAILABILITY

CRL service availability is stipulated in section 4.9.7 (CRL Issuance Frequency).

OCSP service availability is stipulated in section 4.9.9 (On-line Revocation/Status Checking Availability).

4.10.3 OPTIONAL FEATURES

No stipulation.

4.11 END OF SUBSCRIPTION

Stipulated in section 4.9.1(Circumstances for Revocation) and archived as per the CPS.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

The CA maintains its own key escrow.

The CA shall not participate in the third party escrow of private keys.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The TBS *Directive on Departmental Security Management* (Reference O) states that Departments are responsible for selecting, implementing, monitoring and maintaining sustainable security controls to achieve the security control objectives.

5.1.1 SITE LOCATION AND CONSTRUCTION

The CA shall ensure that the location of the computing facilities hosting CA services, including automated registration authorities, will:

a) Satisfy, at a minimum, the requirements for a physical Security Zone; and
b) Be manually or electronically monitored for unauthorized intrusion at all times.

If a non-automated RA is permitted to submit on-line requests in a session with the CA, the CA will ensure the operation of the RA site provides appropriate security protection of the cryptographic module and the RA Administrator's private key.

The RA must ensure that a threat and risk assessment is conducted regarding the crypto module to ensure adequate protection. For example, the cryptographic module and the RA Administrator's private key could be stored in a secure container or safe when not in use.

5.1.1.1 LEVEL 0 ASSURANCE

There is no requirement for protection of an RA workstation associated with **Level 0** assurance.

5.1.1.2 LEVEL 1 ASSURANCE

For **Level 1** assurance, RA workstations must be located in a Restricted Zone or Operations Zone with all media securely protected when unattended.

5.1.1.3 LEVEL 2 ASSURANCE

For **Level 2** assurance, non-automated RA workstations must be located in a Restricted Zone or Operations Zone, with all media securely protected when unattended.

5.1.1.4 LEVEL 3 ASSURANCE

For **Level 3 Assurance**, non-automated RA workstations must be located in a Restricted Zone or an Operations Zone while attended, with all media securely protected when unattended.

5.1.2 PHYSICAL ACCESS

Details on the Physical Controls for site location and construction shall be included in the CPS. Reference TBS Operational Security Standard on Physical Security

5.1.2.1 PHYSICAL ACCESS TO CA EQUIPMENT

Physical access to CA equipment shall be limited to authorized personnel only. At a minimum, physical access controls for CA equipment and all copies of the CA cryptographic module shall meet the following requirements:

a) No unauthorized access to the hardware is permitted;
b) Manual or electronic monitoring for unauthorized intrusion at all times;
c) A site access log is maintained and inspected regularly;
d) Personnel not on the access list are properly escorted and supervised; and
e) Require two-person physical access control to both the computer system and the cryptographic module.

The CA shall ensure all removable CA cryptographic modules, removable media and documents containing sensitive plaintext information are stored in containers either listed in, or of equivalent strength to those listed in, the *Security Equipment Guide* (Reference P) when not in use.

Where a PIN or password is recorded with respect to any CA or RA site, it must be stored in a security container accessible only by authorized personnel.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product.

The Subscriber’s hardware cryptographic module must be protected physically. This may be done through site protection or by the Subscriber by keeping the hardware cryptographic module with them.

5.1.3 POWER AND AIR CONDITIONING

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

The repositories (containing CA certificates and CRLs) shall be provided with power sufficient for a minimum of 24 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 WATER EXPOSURES

The CA shall ensure that the CA system is adequately protected from water exposures.

Potential water damage from fire suppression systems (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 FIRE PREVENTION AND PROTECTION

The CA shall ensure that the CA system is adequately protected from fire by a fire suppression system.

5.1.6 MEDIA STORAGE

The CA shall ensure that the storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 WASTE DISPOSAL

The CA shall ensure that all media containing sensitive information is sanitized to remove information such that data recovery is not possible, or that all media has been securely destroyed before release for disposal.

CA personnel shall account for the destruction of sensitive information.

5.1.8 OFF-SITE BACKUP

The CA shall ensure that it uses facilities, in a location separate from the CA, for off-site backup and archival. The CA shall ensure that:

a) facilities used for off-site backup and archives have:
   i. The same level of security as the primary CA site; and
   ii. Adequate protection from environmental threats such as temperature, humidity and magnetism; and

b) The transmission and/or transport of material for backup and archiving from the CA to the off-site back-up facilities are done securely.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.
The requirements of this policy are drawn in terms of four roles (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):

1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.

2. *Officer* – authorized to request or approve certificates or certificate revocations.

3. *Audit Administrator* – authorized to view and maintain audit logs.

4. *Operator* – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 Administrator

The administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

Administrators shall not issue certificates to subscribers.

5.2.1.2 Officer

The officer shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

5.2.1.4 Operator

The operator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Registration Authority

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6 Certificate Status Authority (CSA) Roles

A CSA shall have at least the following roles.
The CSA Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CSA;
- Establishing and maintaining CSA system accounts;
- Configuring CSA application and audit parameters, and;
- Generating and backing up CSA keys.

The CSA Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CSA is operating in accordance with its CPS ;

The operator shall be responsible for the routine operation of the CSA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.7 CMS Roles

A CMS shall have at least the following roles.

- The CMS administrator shall be responsible for:
- Installation, configuration, and maintenance of the CMS;
- Establishing and maintaining CMS accounts;
- Configuring CMS application and audit parameters; and
- Generating and backing up CMS keys.
- The CMS Audit Administrator shall be responsible for:
- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CMS is operating in accordance with its CPS.
- The CMS Operator shall be responsible for:
- The routine operation of the CMS equipment; and
- Operations such as system backups and recovery or changing recording media.

5.2.1.8 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.1, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A PKI Sponsor need **not** be a Trusted role, but should have been issued a credential that is equal to or higher assurance level than the credential that they are sponsoring.

5.2.1.9 Trusted Agent

A Trusted Agent is responsible for:

- Verifying identity, pursuant to section 3.2; and
- Securely communicating subscriber information to the RA.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Two or more persons shall be required to perform the following tasks:

- □□CA and CSA Signing key generation;
- □□CA and CSA Signing key activation;
- □□CA and CSA Signing private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Auditor Administrator Role.

It is recommended that multiple persons are assigned to all roles assigned in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual in a trusted role shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.
An individual in a trusted role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) access control, where at least one factor is a hardware token shall be used to log into the Administration Workstation. In addition, the hardware token used must be acceptable for the highest certificate policy OID supported by the associated CA. Also See Section 6.7 for authentication to the PKI enclave.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, shall be enforced either by the CA and RA equipment/software, or procedurally, or by both means.

Individual CA, RA and CSA personnel shall be specifically designated to the four roles defined above in Section 5.2.1, as applicable. Individuals may assume more than one role, except:

- Individuals who assume an Officer role shall not assume an Administrator or Auditor role;
- Individuals who assume an Auditor role shall not assume any other role; and
- Under no circumstances shall any of the four roles perform its own compliance auditor function.

No individual in a trusted role shall be assigned more than one identity.

5.3 PERSONNEL CONTROLS

The CA will ensure that personnel other than employees of the Canada Revenue Agency performing duties with respect to the operation of the CA or an RA, shall enter into employment contracts or otherwise acknowledge the terms and conditions of their engagement. The CA shall ensure that such terms and conditions of employment include a requirement on the part of such personnel to not disclose sensitive CA security-relevant information or private information as that term is defined in Section 9.4.2.

The CA shall ensure that it will not assign duties to personnel that may cause a conflict of interest with their CA or RA duties.

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

The CA shall ensure that staff performing CA and RA functions possesses the necessary knowledge, experience and qualifications to perform their duties.

The CA shall ensure that all personnel associated with either the operation of the CA or who operate an automated registration authority or RA software for the purpose of on-line entity management have a “Secret” security clearance.

5.3.2 BACKGROUND CHECK PROCEDURES

All background checks must be performed in accordance with the *Policy on Government Security (Reference Q)*.

5.3.3 TRAINING REQUIREMENTS

The CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

The CA shall review and update its training program as required to accommodate changes in the CA system.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

In the event of actual or suspected unauthorized actions by a person performing duties with respect to the operation of the CA or an RA, the CA shall suspend his or her access to the CA system.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

The CA shall ensure that contract personnel satisfy the same personnel security requirements with respect to appointment, training and background checks as those applicable to CA employees.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

The CA shall provide a CP, relevant provisions of the CPS, and any specific statutes, policies or contracts relevant to their positions to CA personnel, RAs and DRIs.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CAs, CSAs, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1 TYPES OF EVENTS RECORDED

All security auditing capabilities of the CA, CSA, and RA operating system and their associated applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,

- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,

A message from any source requesting an action by a CA is an auditable event. The message must include message date and time, source, destination and contents.

The following events shall be audited:

Auditable Event	CA	CSA	RA
SECURITY AUDIT			
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X
Obtaining a third-party time-stamp	X	X	X
IDENTITY-PROOFING			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X
LOCAL DATA ENTRY			
All security-relevant data that is entered in the system	X	X	X
REMOTE DATA ENTRY			
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT			

All successful and unsuccessful requests for confidential and security-relevant information	X	X	X
KEY GENERATION			
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of Component private keys	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X
SECRET KEY STORAGE			
The manual entry of secret keys used for authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT			
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All certificate requests	X	N/A	X
CERTIFICATE REVOCATION			
All certificate revocation requests	X	N/A	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request	X	N/A	N/A
CA CONFIGURATION			
Any security-relevant changes to the configuration of the Component	X	X	X
Auditable Event	**CA**	**CSA**	**RA**
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	-	-
The access control privileges of a user account or a role are modified	X	-	-

CERTIFICATE PROFILE MANAGEMENT			
All changes to the certificate profile	X	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT			
All changes to the CSA profile (e.g. OCSP profile)	N/A	X	N/A
REVOCATION PROFILE MANAGEMENT			
All changes to the revocation profile	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			
All changes to the certificate revocation list profile	X	N/A	N/A
MISCELLANEOUS			
Appointment of an individual to a Trusted Role	X	X	X
Designation of personnel for multiparty control	X	-	N/A
Installation of the Operating System	X	X	X
Installation of the PKI Application	X	X	X
Installation of hardware cryptographic modules	X	X	X
Removal of hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System Startup	X	X	X
Logon attempts to PKI Application	X	X	X
Receipt of hardware / software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Back up of the internal CA database	X	-	-
Restoration from back up of the internal CA database	X	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-
Posting of any material to a repository	X	-	-
Access to the internal CA database	X	X	-
Auditable Event	**CA**	**CSA**	**RA**
All certificate compromise notification requests	X	N/A	X
Loading tokens with certificates	X	N/A	X
Shipment of Tokens	X	N/A	X

Zeroizing Tokens	X	N/A	X
Re-key of the Component	X	X	X
CONFIGURATION CHANGES			
Hardware	X	X	-
Software	X	X	X
Operating System	X	X	X
Patches	X	X	-
Security Profiles	X	X	X
PHYSICAL ACCESS / SITE SECURITY			
Personnel Access to room housing Component	X	-	-
Access to the Component	X	X	-
Known or suspected violations of physical security	X	X	X
ANOMALIES			
Software error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages	X	X	X
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	-	-
Electrical power outages	X	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-
Obvious and significant network service or access failures	X	-	-
Violations of Certificate Policy	X	X	X
Violations of Certification Practice Statement	X	X	X
Resetting Operating System clock	X	X	X

5.4.2 FREQUENCY OF AUDIT LOG PROCESSING

The CA shall ensure that CA personnel review audit logs on a regular basis:

a) For **Level 0** assurance there is no requirement to review logs.
b) For **Levels 1 and 2** assurance audit logs must be reviewed weekly.
c) For **Level 3 Assurance** audit logs must be reviewed daily.

Such reviews involve verifying that the log has not been tampered with, and then inspecting all log entries. Initial review of audit logs may be automated. CA personnel shall conduct a more thorough investigation of any “alerts” or irregularities in the logs. All significant events discovered in the review of the log files must be explained in an audit log summary.

The CA shall indicate who has responsibility for audit log review and audit log summary preparation in the CPS.

The CA should examine supporting manual and electronic logs, including those from RAs, where any action is deemed suspicious.

The CA shall document any actions taken following these reviews.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The CA shall retain its audit logs on site for at least two (2) months and subsequently retain audit logs generated by the PKI software in the manner described in Section 5.5.

5.4.4 PROTECTION OF AUDIT LOG

The CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 AUDIT LOG BACK-UP PROCEDURES

The CA shall back up, if in paper form, all audit logs and audit summaries.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS EXTERNAL)

The CA shall identify its audit collection systems in the CPS.

5.4.7 NOTIFICATION OF EVENT CAUSING SUBJECT

Where an event is logged by the audit collection system, the CA reserves the right not to provide notice to the individual, role, device or application that caused the event.

5.4.8 VULNERABILITY ASSESSMENTS

Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA shall ensure that a vulnerability assessment is performed, reviewed and revised:

a) following an examination of these monitored events; or
b) on a periodic basis.

The CA shall take appropriate action to minimize identified system vulnerabilities as soon as reasonably possible.

5.5 RECORDS ARCHIVAL

In addition to the following sub-sections, information retained or backed up by the CA may be subject to archival requirements, pursuant to the *Library and Archives of Canada Act (Reference R)*, other applicable legislation and GC policy.

5.5.1 TYPES OF RECORDS ARCHIVED

CA, CSA, and RA archive records shall be sufficiently detailed to establish the proper operation of the PKI or the validity of any certificate (including those revoked or expired) issued by the CA.

Data To Be Archived	CA	CSA	RA
Certification Practice Statement	X	X	X
Certificate Policy	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	-
Modifications and updates to system or configuration	X	X	-
Certificate requests	X	-	-
Revocation requests	X	-	-
Subscriber identity authentication data as per Section 3.2.3	X	N/A	X
Documentation of receipt and acceptance of certificates, including subscriber agreements	X	N/A	X
Documentation of receipt of Tokens	X	N/A	X
All certificates issued or published	X	N/A	N/A
Record of component CA Re-key	X	X	X
All CRLs and CRLs issued and/or published	X	N/A	N/A
All Audit Logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X
Compliance Audit Reports	X	X	X

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention period for archive data is 10 years and 6 months for level 1 & 2 Assurance levels. The minimum retention period for archive data is 20 years and 6 months for level 3 assurance level.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 PROTECTION OF ARCHIVE

Confidentiality private keys backed up by the CA shall be protected at a level of physical and cryptographic protection equal to or exceeding that in place at the CA site.

A second copy of all material retained or backed up must be stored in a location other than the CA site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4 ARCHIVE BACKUP PROCEDURES

A second copy of all material retained or backed up must be stored in a location other than the CA site.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Archive records shall be automatically time-stamped as they are created. The CPS shall describe how the system clocks used for time-stamping are maintained in synchrony with an authoritative time source.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

The CA shall verify the integrity of back-ups and the integrity of materials stored off-site once every year

5.6 KEY CHANGEOVER

Automatic key changeover (renewal) is not supported.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

5.7.1.1 CA KEY COMPROMISE

CRA PKI PMA shall be notified if any CAs operating under this policy experiences the following:

a) suspected or detected compromise of the CA systems;
b) physical or electronic penetration of CA systems; or
c) any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

In the event of the compromise of the CA’s private digital signature key and prior to its re-generation, the CA shall immediately:

a) Notify parties as per CA Public Certificate Revocation;
b) Request revocation of cross-certificates issued to the CA; and
c) Revoke all certificates issued using that key.

CA Public Certificate Revocation

In the event of the need for revocation of the CA's Digital Signature certificate, the CA must immediately notify:

a) The CRA PKI PMA;
b) All CAs to whom it has issued cross-certificates, including the CFPB (bridge) as that would be the most common only point of cross-certification;
c) All of its RAs;
d) All Subscribers;
e) All DRIs; and
f) All Application Responsible Owners.

The CA shall publish the certificate serial number on an appropriate ARL and revoke all cross-certificates signed with the revoked CA Digital Signature certificate.

After addressing the factors that led to revocation, the CA may generate a new CA signing key pair and re-issue certificates to all Subscribers, ensuring that all CRLs and ARLs are signed using the new key.

The CA shall indicate in the CPS or in a publicly available document and appropriate agreements how it will provide notice of CA public revocation of its signing key.

5.7.2 COMPUTING RESOURCES, SOFTWARE AND/OR DATA ARE CORRUPTED

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

a) Before returning to operation, ensure that the system's integrity has been restored.
b) If the CA signature keys are not destroyed, CA operation shall be re-established, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
c) If the CA signature keys are destroyed, CA operation shall be re-established as quickly as possible, giving priority to the generation of a new CA key pair.

The CA will state in the CPS, or other appropriate documentation, procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data.

Where a repository is not under the control of the CA, the CA shall ensure any agreement or arrangement with the repository provides that the repository establish and document procedures to address the corruption or loss of the repository's computing resources, software and/or data.

5.7.3 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The CA shall prepare and maintain a business continuity plan as per the *Operational Security Standard - Business Continuity Planning (BCP) Program* (Reference Y*)* outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster.

Where a repository is not under the control of the CA, the CA must ensure that any agreement or arrangement with the repository provides that the repository establish and document a business continuity plan.

5.8 CA OR RA TERMINATION

In the event the CA ceases operation or makes a major change in operations, the CA shall immediately notify:

a) The CRA PKI PMA;
b) All CAs to whom it has issued cross-certificates;
c) All of its RAs;
d) All Subscribers;
e) All DRIs; and
f) All Application Responsible Owners.

Upon the de-commissioning of the CA, all CA private keys that have ever been, or potentially could be used for continued CA cryptographic operations shall be revoked (by reason of cessation of service) and destroyed in accordance with section 6.2.10 (Method of Destroying Private Key). A final CRL and ARL shall be generated and published.

In the event the CA ceases operations, the CA shall arrange for the retention of the CA's records by an authorized custodian, including two copies of:

a) Certificates;
b) Confidentiality private keys (if applicable);
c) Cross-certificates;
d) CA self-signed certificates;
e) ARLs and CRLs;
f) Audit information detailed in Section 5.4; and
g) Other records that have been archived as detailed in section 5.5, in accordance with archival requirements specified in this Certificate Policy.

The CA shall also arrange for the retention of any data (e.g., passwords) required to ensure that CA records are usable (e.g., encrypted data can be decrypted at a later date where required).

The secure transfer shall be conducted as per section 5.1.8 (Off-site Backup).

Practice note: This does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs. Such CA's are required to continue to conform to all relevant aspects of this policy (such as Audit logging and archive).

6 TECHNICAL SECURITY CONTROLS

The CA shall secure all CA operations using mechanisms such as strong authentication and encryption when accessed across a shared network.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY GENERATION

The CA shall ensure that CA key generation shall be:

a) Performed by personnel in trusted roles under, at a minimum, dual control;
b) Carried out within a device which satisfies the requirements identified in Section 6.2.1 or higher; and
c) Performed using a GC CSE approved algorithm.

The CA must document its CA key generation procedures and generate auditable evidence that the documented procedures were followed.

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140-2 validated cryptographic modules. The module(s) shall meet or exceed FIPS 140-2 Level 2. Multiparty control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

> Practice note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with corrective actions taken, the key generation process need not be restarted but may continue.

6.1.1.2 SUBSCRIBER KEY GENERATION

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For Level 3 assurance level certificate type, subscriber key pairs shall be generated in FIPS 140-2 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a random bit generator whose output is directly from or combined with the output of a CSE-approved Deterministic Random Bit Generator (DRBG) listed in ITSP.40.111. (Reference Z).

6.1.1.3 CSS KEY PAIR GENERATION

Cryptographic keying material used by CSSs to sign status information shall be generated in FIPS 140 validated cryptographic modules. The cryptographic module(s) shall meet or exceed FIPS 140-2 Level 2.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgment of receipt of the token.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

If the CA does not generate the public verification key, the CA shall arrange for its delivery to the CA, in a secure manner, as documented in an applicable IETF standard such as RFC 4210 (CMP) or RFC 5272 (CMC).

If the CA does not generate the public encryption key, the CA shall arrange for its delivery to the CA, in a secure manner, as documented in an applicable IETF standard such as RFC 4210 (CMP) or RFC 5272 (CMC).

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in cross-certificates.
Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms; such as
  - The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.
  - The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token, which is then delivered to the subscriber in accordance with section 6.1.2.
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

Practice note: other methods that preclude substitution attacks may be considered acceptable.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

Practice note: the key rollover certificates must be distributed using repositories. Moreover, if a specific notification procedure has been reached with a relying partner such as a cross certified CA, then these procedures must be adhered to in addition to publication in a repository.

6.1.5 KEY SIZES

The use of a specific key size must follow ITSP.40.111.

This CP requires use of RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

CA keys and subscriber keys using RSA must adhere to minimum module length as per ITSP.40.111. CA keys and subscriber keys using ECDSA must adhere to minimum field sizes as per ITSP.40.111.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public key parameters shall always be selected from the set specified in section 7.1.3.

6.1.7 KEY USAGE PURPOSES (AS PER X.509V3 KEYUSAGE FIELD)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a key usage extension.

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both. User certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. Where the subject signs OCSP responses, the certificate shall assert the *digitalSignature* and/or *nonRepudiation* bits. (This certificate shall be issued directly to the responder by the cognizant CA).

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

6.2.1.1 CA CRYPTOGRAPHIC MODULES

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated as specified in FIPS 140-2 level 3 or otherwise deemed to provide an equivalent level of functionality and assurance.

All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-2 Level 3 or otherwise deemed to provide an equivalent level of functionality and assurance.

6.2.1.2 RA CRYPTOGRAPHIC MODULES

RAs Digital Signature key generation and signing operations must be performed in a hardware cryptographic module which is rated to at least FIPS 140-2 Level 3, or otherwise deemed to provide an equivalent level of functionality and assurance.
Automated registration processes may be performed in a software cryptographic module rated to at least

FIPS 140-2 Level 2 or otherwise deemed to provide an equivalent level of functionality and assurance, if the CA is satisfied that the physical security of the software is adequate.

6.2.1.2.1 Level 0 Assurance

No stipulation.

6.2.1.2.2 Levels 1 and 2 Assurance

All other RA cryptographic operations must be performed in cryptographic modules rated at FIPS 140-2 Level 1.

6.2.1.2.3 Level 3 Assurance

All other RA cryptographic operations must be performed in cryptographic modules rated at FIPS 140-2 Level 3.

6.2.1.3 END ENTITIES CRYPTOGRAPHIC MODULES

All cryptographic modules must automatically lock after a specific period of inactivity, as stipulated in the CPS.

6.2.1.3.1 Level 0 Assurance

No stipulation.

6.2.1.3.2 Levels 1 and 2 Assurance

End Entities must use cryptographic modules validated to:

a) FIPS 140-2 Level 1; or
b) an equivalent level of functionality and assurance.

6.2.1.3.3 Level 3 Assurance

End Entities must use cryptographic modules validated to:

a) FIPS 140-2 Level 2; or
b) an equivalent level of functionality and assurance.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

There must be multi-person control for CA key generation operations. Two individuals, one of whom performs the duties associated with the role of PKI Admin User, must participate or be present.

There must be multi-person control for issuance or lifecycle management of keys to Trusted Roles. Two individuals, one of whom performs the duties associated with the role of PKI Security Officer must participate or be present.

The Subscriber may be permitted to securely perform key recovery or revocation operations. When not performed by the Subscribers themselves, there must be multi-person control for Subscriber private key recovery of the Subscriber. Two individuals, one of whom is a PKI Security Officer or RA, must participate or be present.

6.2.3 PRIVATE KEY ESCROW

The CA shall not participate in the third party escrow of private keys.

6.2.4 PRIVATE KEY BACK-UP

6.2.4.1 CA KEY STORAGE, BACKUP AND RECOVERY

The CA shall ensure that the CA private keys remain confidential and maintain their integrity. In particular:

a) The CA private signing key shall be held and used within a secure cryptographic device that meets the requirements identified at Section 6.2.1;
b) The CA private signing key may be exported in any manner approved by CSE from one cryptographic device to any other cryptographic device that meets the requirements of Section 6.2.1;
c) When outside the signature-creation device, the CA private signing key shall be encrypted;
d) The CA's private signing key shall be backed up, stored and recovered under the same multi-person control as the original key, such backup being securely stored at the CA backup location; and
e) Where the CA keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

The CA shall indicate in the CPS its key back-up procedures.

6.2.4.2 SUBSCRIBER KEY BACKUP

A Subscriber may back-up his/her own private decryption keys at LOA 1 and 2(soft certificate) and NOT for LOA 3.

If so, the keys must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

As a normal course of business, the CA shall back up the private decryption keys of its Subscribers. On an exception basis, the CA may not back up the private decryption keys for some of its Subscribers.

Backed-up keys must be stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

6.2.5 PRIVATE KEY ARCHIVAL

Refer to Section 0.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

If a private signature key is not generated in the Subscriber's cryptographic module, it must be entered into the module in a secure manner using PKIX CMP or equivalent secure protocol. If the private key is generated by an issuing terminal (such as for a SmartCard), the system should be evaluated to ensure that it has the require assurance to ensure that the keys are properly destroyed after programming and are never exported from the terminal other than to the destined cryptographic container. IT IS NOT RECOMMENDED TO GENERATE SIGNATURE KEYS OUTSIDE THE Subscriber cryptographic module.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

Private keys shall be stored in a “secure container”, as specified in *Operational Security Standard on Physical Security* (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12329).

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

A Subscriber must be authenticated to the “secure container” storing the private key, before the activation of the private key. The CA shall ensure that password policy rules are in place to require the use of strong passwords to access a “secure container”.

The CRA PKI may approve other authentication methods for the activation of private keys

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity, as defined in the applicable CPS.

When private keys are deactivated, they must be cleared from memory before the memory is de-allocated and must be kept in encrypted form only.

Any disk space where keys were stored must be over-written before the space is released to the operating system.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Upon the termination of use, the holder of a private key must securely destroy all copies of that key in computer memory and in shared disk space.

For software cryptographic modules, this can be done by deleting the data. For hardware cryptographic modules, this can likely be done by executing a “zeroize” command. Physical destruction of hardware tokens is not required.

6.2.11 CRYPTOGRAPHIC MODULE RATING

As per section 6.2.1 (Cryptographic Module Standards and Controls)

6.3 OTHER ASPECTS OF KEY PAIRMANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

The CA shall retain all digital signature verification public key certificates it generates.

The CA shall retain all encryption public key certificates it generates.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

The usage period for the PersonUser Policy Root CA key pair is a maximum of 10 years.

The CA private key may be used to sign certificates for at most four years, but may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair’s usage period.

For OCSP responders operating under this policy, the maximum usage period is three years.

Level 1 and 2 assurance certificates can have an expiry date of up to four years from creation.

Level 3 assurance certificates can have an expiry date of up to three years from creation.

Subscriber signature private keys have the same usage period as their corresponding public key.

6.4 ACTIVATION DATA

Practice note: the CA will be operational for a period of 10 years but it can only issue user certificates for a maximum of six years (for levels 1 and 2). This means that during the fourth year of operation a root key ceremony is required to create a new root key. Cross over certificates will be made and published.

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

Any activation data must be unique and unpredictable.

Keys and initialization data may be generated in bulk and shall be held by the CA in a secure manner prior to distribution. The secure manner shall be appropriate for the sensitivity of the information the keys will ultimately protect – Level of Assurance 2 or below certificates should protect this data in a fashion similar to password databases, Level of Assurance 3 data should use approved cryptographic protection at rest with encryption keys stored in an HSM or an equivalent level protection through the use of physical and operational compensating controls. Upon receipt of initialization data, a Subscriber must use the initialization data in a timely manner.

6.4.2 ACTIVATION DATA PROTECTION

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

6.5.1.1 LEVEL 0 ASSURANCE

No stipulation.

6.5.1.2 LEVELS 1 AND 2 ASSURANCE

The CA server must include the following security functionality:

a) Access control to CA services and PKI roles;
b) Enforced separation of duties for PKI roles;
c) Identification and authentication of PKI roles and associated identities;
d) Object reuse controls or separation for CA random access memory;
e) Where required, use of cryptography for session communication and database security;
f) Archival of CA and Subscriber history and audit data;
g) Audit of security related events;
h) Automatic and regular validation of CA database integrity;
i) Trusted path mechanisms for the identification and authentication of PKI roles and associated identities;
j) Recovery mechanisms for keys and the CA system; and
k) Hardening of the CA's operating system.

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software and physical safeguards.

6.5.1.3 LEVEL 3 ASSURANCE

In addition to having the security functionality required for levels 1 and 2 assurance, the CA server shall also enforce domain integrity boundaries for security critical processes.

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software and physical safeguards.

6.5.2 COMPUTER SECURITY RATING

No Stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The CA must use CA software that has been designed and developed under a structured development methodology.

The design and development process must provide sufficient documentation to support third party verification of process compliance, third party security evaluation of the CA components and ongoing Threat Risk Assessments in order to influence security safeguard design and minimize residual risk.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container or in another trustworthy manner and be installed by trained personnel.

6.6.2 SECURITY MANAGEMENT CONTROLS

The CA hardware and software shall be dedicated to performing only CA-related tasks. There must be no other applications, hardware devices, network connections or component software, which are not part of the CA operation.

The CA shall indicate in the CPS its policies and procedures to prevent malicious software from being loaded onto the CA equipment. CA and RA as well as automated registration software shall be scanned for malicious code on first use and periodically afterward.

The CA shall use formal configuration management methodology for the installation and ongoing maintenance of the CA system. The CA software, when first loaded, must provide a method for the CA to verify that the software on the system:

a) Originated from the software developer;
b) Has not been modified prior to installation; and
c) be the version intended for use.

The CA shall provide a mechanism to periodically verify the integrity of the CA database. The CA will also have mechanisms and policies in place to control and monitor the configuration of the CA system.

6.6.2.1.1 Level 0 Assurance

No stipulation.

6.6.2.1.2 Levels 1 and 2 Assurance

Upon installation, the integrity of the CA database must be validated, at minimum, once a week.

6.6.2.1.3 Level 3 Assurance

Upon installation, the integrity of the CA database must be validated every 24 hours.

6.7 NETWORK SECURITY CONTROLS

The CA shall ensure that security controls are put in place to provide CA integrity and availability through any open or general purpose network with which it is connected. Such protection must include the installation of one or more devices configured to allow only the protocols and, at the option of the CA, those commands required for CA operations. Any network software present must be necessary to the functioning of the CA operation.

The CA shall state in its CPS such protocols and, if required, commands required for the operation of the CA.

6.8 TIME-STAMPING

The CA may provide, or cause to be provided, to Subscribers the capability to time-stamp their transactions.

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, or a later version of X.509 certificates if such use is approved by the CSE.

7.1.2 CERTIFICATE EXTENSIONS

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles.

Certificate extensions used by certificates issued under this Certificate Policy shall conform to the applicable parts of the *PKI X.509 Certificate and CRL Fields and Extensions standard (*RFC 5280) (Reference N).

The CAs shall post its CA's Profile of Base Fields and Extension Fields of X.509 Certificates and CRLs on a web site and advise Subscribers of its location.

Critical private extensions shall be interoperable in their intended community of use.

Where private extensions are used, they shall be identified in its CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Certificates issued under this CP shall use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID shall be used to specify the hash in an RSASSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2)

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4 NAME FORMS

The subject field of certificates issued under this policy shall be populated with an X.500 distinguished name as specified in section 3.1.1.

7.1.5 NAME CONSTRAINTS

The CA may assert name constraints in CA certificates.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

In addition to the policy document object identifier, certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-cra-certpcy-Level_0-PersonUser	2.16.124.101.1.272.3.#.1.0
id-cra-certpcy-Level_1-PersonUser	2.16.124.101.1.272.3.#.1.1
id-cra-certpcy-Level_2-PersonUser	2.16.124.101.1.272.3.#.1.2
id-cra-certpcy-Level_3-PersonUser	2.16.124.101.1.272.3.#.1.3

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

The CAs may assert policy constraints in CA certificates.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 PROCESSING SEMANTICS FOR CRITICAL CERTIFICATE EXTENSIONS

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2 CRL PROFILE

7.2.1 VERSION NUMBER(S)

The CA shall issue X.509 version 2 CRLs and ARLs, or a later version of X.509 CRLs and ARLs if such use is approved by the CSE.

The CA shall state in its CPS the use of any extensions supported by the CA, its RAs and End Entities.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

All Subscriber PKI software must correctly process all:

CRL extensions including: authorityKeyIdentifier, issuerAltName, cRLNumber, deltaCRLIndicator, and issuingDistributionPoint; and

CRL Entry Extensions: reasonCode, holdInstructionCode, invalidityDate, and certificateIssuer.

The CA shall state in its CPS the use of all extensions supported by the CA, its RAs and End Entities.

7.3 OCSP PROFILE

7.3.1 VERSION NUMBER

If the use of OCSP servers is approved by The CRA PKI PMA, the CA shall comply with the IETF RFC2560 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Version 1 (Reference S)*.

7.3.2 OCSP EXTENSIONS

If the use of OCSP servers is approved by the CRA PKI PMA, the CA must state in its CPS the use of any OCSP extensions supported by the CA, its RAs and Subscribers.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A compliance audit determines whether the CA's performance meets the requirements established by this Certificate Policy and associated CPS.

As part of the SA&A process a compliance audit of the CA will be conducted on such terms and conditions as may be established by the CRA PKI PMA for CRA PKI CA.

As part of the cross-certification process with the CFPB, the CA shall provide to TBS, CIOB the results of any compliance audit conducted as part of that process.

Compliance audit reports shall not be made public unless required by law pursuant to judicial authorization or an express statutory requirement or by an agreement.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The CA will have a compliance inspection conducted at least annually.

A qualified professional external to the CA shall conduct one (1) of every three (3) audits of the CA. TBS, CIOB may order a compliance audit by an agency external to the CA at any time.

TBS, CIOB, at its discretion, may request the Deputy Minister responsible for the CA to have a compliance audit by an agency external to the department at any time.

The CA will certify annually to TBS, CIOB that they have at all times during the period in question complied with the requirements of this Certificate Policy and will provide reasons where it has not complied with this Certificate Policy and state any periods of non-compliance.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of PKI security assessments, and must be familiar with the requirements that TBS, CIOB imposes on the issuance and management of certificates issued under this Certificate Policy.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor must be independent of the management or operation of the CA.

An auditor who is external to the Government of Canada must be independent of the CA and, if applicable, must comply with the provisions of the *Conflict of Interest and Post-Employment Code for the Public Service (Reference X)*.

8.4 TOPICS COVERED BY ASSESSMENT

At a minimum, the scope of a compliance audit will include whether:

a) The CPS outlines, in sufficient detail, the technical, procedural and personnel practices of the CA required under this Certificate Policy;
b) The CA implements and complies with those technical, procedural and personnel practices; and
c) The Repository Manager, RAs and LRAs implement and comply with the technical, procedural and personnel practices set out by the CA.

An auditor may consult with Application Responsible Owners to determine relevant applications, procedures and practices, which may have a bearing on the audit.

TBS, CIOB or CRA PKI PMA may increase the scope of a compliance audit on such terms as it deems appropriate.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The audit results will be submitted to the accreditation authority of the CA. If irregularities are found, the CA will submit a report to the accreditation authority as to any action the CA will take in response to the inspection report.

Where a CA fails to take appropriate action in response to the audit report, the authorization authority may:

a) Indicate the irregularities, but allow the CA to continue operations until the next programmed audit;
b) Allow the CA to continue operations for a maximum of thirty (30) days pending correction of any problem prior to revocation;
c) Downgrade the assurance level of the cross-certificate with the CFPB; or
d) Revoke the CA's certificate.

Where the authorization authority fails to take appropriate action, TBS, CIOB may:

a) Downgrade the assurance level of the cross-certificate with the CFPB; or
b) Revoke the CA's cross certificate with the CFB.

Any decision regarding which of these actions to take will be based on the severity of the irregularities.

8.6 COMMUNICATION OF RESULTS

Audit information is to be considered sensitive and must not be disclosed for any purpose other than inspection purposes or where required by agreement or by law pursuant to judicial authorization or an express statutory requirement.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

The charging of fees for the issuance and management of certificates and CRLs is subject to appropriate legislative authority and policy. The CA shall not charge fees to Subscribers or Relying Parties without TBS, CIOB approval.

In the event fees are charged, notice of any fee will be given and no fee shall be charged unless and until notice is given to Subscribers and Relying Parties, as appropriate, and an opportunity to discontinue receiving CA services is given.

The charging of fees in relation with the enrolment in, or the use of services from a Program is outside the scope of this policy. Such fees are determined and implemented by the authorized departmental or agency personnel.

9.1.2 CERTIFICATE ACCESS FEE

No stipulation.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

No stipulation.

9.1.4 FEES FOR OTHER SERVICES

No stipulation.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Business Confidential information from an organization is deemed Private for the purposes of information protection.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

No stipulation.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

Business confidential information associated with the issuance of certificates under this Certificate Policy is considered particularly sensitive and therefore must be labelled PROTECTED B.

9.4 PRIVACY OF PERSONAL INFORMATION

Personal information collected for identification and authentication is protected under the provisions of the *Privacy Act (Reference T)*..

9.4.1 PRIVACY PLAN

The sensitivity of private information held by departments in connection with certificates issued under this Certificate Policy varies and is determined by reference to:

a) Applicable statutes and regulations, including but not limited to the *Privacy Act(Reference* T*), Access to Information Act (Reference U)* and *Library and Archives of Canada Act (Reference R)*;
b) Applicable government security policies; and
c) Applicable government privacy policies.

9.4.2 INFORMATION TREATED AS PRIVATE

Private information includes:

a) identifiable information about an individual; and
b) business confidential information from an organization.

The CA shall not collect private information for any purpose other than the issuance and management of certificates to personnel of a Program, the CA or any CA service provider, RA or Subscriber. The CA shall not collect any more information than is necessary for that purpose.

The owner of private information or a Designated Organization where applicable, may correct any inaccuracies or request any corrections in the private information provided by the owner at any time. The CA and any RA will designate an individual to be responsible to receive any requests to correct PKI-related private information and will publish contact information on its web site or in any appropriate manner in particular circumstances.

Private information held by departments or agencies, in connection with programs for which certificates have been issued under this Certificate Policy is subject to applicable program legislation and policies. Opportunities to correct such information will be determined by the Program Business Manager.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Certificate revocation/suspension information, including reason codes, may be included in a CRL entry. Certificates and CRLs are not considered private information for the purposes of this Certificate Policy.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Private information associated with the issuance of certificates under this Certificate Policy is considered particularly sensitive and therefore must be labelled PROTECTED B.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

The CA shall ensure that any application for a certificate to be issued by the CA contains language to obtain the consent of the applicant for the use and disclosure of private information as outlined in this Certificate Policy and in any agreement.

The CA shall only use private information collected by the CA or RA for the purpose of issuing and managing a certificate under this Certificate Policy.

The use of private information collected by Departments, in connection with Programs, which are to use certificates issued under this Certificate Policy, is determined by departmental and agency Program Business Managers responsible for the program or service in question and may vary depending upon the application in question.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

The CA or any RA shall only release private information, collected for the purpose of issuing and managing a certificate, to law enforcement officials or where requested to do so in connection with legal proceedings. Release shall occur only upon receipt of:

a) a judicial order;
b) the consent of the owner of the private information; or
c) where required or permitted pursuant to express statutory authority.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Subject to Sections 9.4.5 and 9.4.6 and the limitations and permissions imposed by the *Privacy Act (Reference T)* and other applicable statutes, regulations and policies, and in consultation with the Departmental ATIP Coordinator, the CA and any RA may distribute private information only to personnel of departments or agencies that require such information to assist in the issuance and management of certificates.

The CA or any RA may release private information if, in the opinion of the CA or RA, there is a life-threatening emergency.

Any release of program specific private information is governed by applicable statutes and policies.

9.5 INTELLECTUAL PROPERTY RIGHTS

All right, title and interest in all intellectual property rights in or associated with

As specified in Section 2.1, all CA certificates shall be published in repositories.
This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3., CRLs, ARLs, Distinguished Names, Service Arrangements, CA Public Keys and certificates as well as Subscriber's certificates (the "Materials"), including all modifications and enhancements thereof, are and shall remain the exclusive property of the CRA.

Subscribers and Relying Parties may use the Materials only for the purposes of complying with this Certificate Policy. Any other commercial or non-commercial use is strictly prohibited. The CP may be copied and distributed provided all copyright or other proprietary notices, if included, are retained or an equivalent acknowledgment is provided as to its origin and ownership.

Any software provided in conjunction with the use of the Materials is the property of the CRA or its third party licensors. The use of any such software shall be in accordance with the terms of the license applicable to the software.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

The CA is responsible for:

a) The creation and signing of certificates binding Subscribers, CA personnel and (where permitted) other CAs with their public verification keys; and
b) Promulgating certificate status through CRLs and ARLs.

The CA may also generate Subscriber Digital Signature key pairs when using automated registration processes.

The CA shall:

a) Operate for the purpose of issuing and managing certificates for Subscribers, CA personnel, RAs and Repository Managers, as required, and issuing and managing cross-certificates in accordance with this Certificate Policy, the applicable CPS, applicable laws of Canada, and policies of the Government of Canada;
b) Prepare a detailed CPS describing all practices, procedures and requirements required to comply with this Certificate Policy;
c) Ensure that all RAs and Repository Managers acting on its behalf operate in accordance with these CPs and the applicable CPS;
d) Ensure that appropriate agreements or arrangements outlining the respective rights, privileges and obligations of the parties are entered into with:
    i. Subscribers for certificates issued to them or on their direction; and
    ii. All others who perform functions on behalf of the CA.
e) Provide, in a publicly available document, such information as applicants for certificates may require to request the issuance of a certificate, its suspension or revocation;
f) Endeavour to provide Subscribers and Relying Parties with notice of their respective rights, privileges and obligations pertaining to their use of any PKI keys, certificates, hardware or software provided by the CA;
    i. Notify LRA when a certificate for their use is issued.
g) Provide notice in certificates issued under these policies of the address of the CRL;

h) Provide appropriate notice to all interested parties as to the CA's procedures concerning the expiration, suspension, revocation and renewal of certificates;
i) Make revocation information available to a Subscriber or Relying Party as required under this CP;
j) Use its private signing key only to sign certificates and CRLs and for no other purpose;
k) Institute procedures to ensure CA personnel associated with PKI roles (e.g. PKI Admin User; PKI Security Officers, and PKI Administrators) are accountable for actions they perform and ensure evidence is available to link any action to the person performing such action;
l) Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes;
m) Subject to applicable laws and policies of Canada, ensure that the information held by the CA or on behalf of the CA is stored in Canada;
n) Except as otherwise stipulated, publication of a certificate in a repository constitutes the CA's certification, and notice to a Subscriber or a Relying Party who may access the certificate in the repository, that the information stated in the certificate was verified in accordance with this Certificate Policy;
o) Ensure that it puts mechanisms in place to minimize the amount of time the CA services are unavailable to Subscribers; and
p) Embed a notice of limitations of liability within the certificates it creates. Because of space limitations within a certificate, such notice must be limited to the following language: "Limited Liability. See CP.-Responsabilité limitée. Voir PC. "

When required as a result of the technology used (e.g. roaming profiles), the CA shall place Subscriber private keys in protected Storage.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

The RA shall:

a) Comply with applicable provisions of these CPs and CPS, and with the terms and conditions of any agreement or arrangement with the CA;
b) Inform applicants of the application process, including the process for the initialization of certificates;
c) Prior to certificate issuance, identify and authenticate the identities of applicants seeking to become Subscribers and, when submitting application information to the CA, certify to the CA that it has done so in accordance with the requirements of this Certificate Policy;
d) Inform Subscribers of:
    i. Their respective rights, privileges and obligations pertaining to their use of any PKI keys, certificates, hardware or software provided by the CA; and
    ii. The CA's procedures for the expiration, suspension, revocation and renewal of keys and certificates;
e) Ensure for audit purposes, that records of actions carried out in performance of RA duties are maintained, if the CA does not record the information; and
f) Protect the RA's private keys as directed by the CA.

RAs may support both automated on-line and off-line registration processes.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

An individual may request a certificate for use on their own behalf or on behalf of another individual other than themselves with appropriate verifiable authorization. In these cases, the Subscriber obligations are extended to the individual authorized to act on behalf of the Subscriber.

A Subscriber shall:

a) Ensure that information submitted to the CA or RA directly or on their behalf is complete and accurate;
b) Comply with the terms of:
   i. A PKI Employee Use Policy in the case of CRA or CBSA Employees; or
   ii. A Subscriber Agreement or other binding instrument satisfactory to the CA;
c) Use or rely on keys or certificates only for purposes permitted by this Certificate Policy and for no other purpose;
d) Perform intended cryptographic operations using appropriate software and hardware;
e) Protect their private keys, passwords and key tokens (if applicable) in such manner as set out in this Certificate Policy or as directed and take all reasonable measures to prevent their loss, disclosure, modification or unauthorized use;
f) Not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered);
g) Assume responsibility for the protection of any information following its decryption and/or verification, especially where the Subscriber chooses to re-encrypt information for storage purposes;
h) Immediately notify the CA in such manner as specified by the CA in the event of the compromise or suspected compromise of a Subscriber's private keys, password or key tokens (if applicable); and
i) With respect to the use outside of Canada of hardware or software containing cryptographic products or elements, verify that the:
j) Importation and/or use of such products is permitted within a particular country or jurisdiction; and
k) Exportation of such products from Canada to another country or jurisdiction is permitted.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

A Relying Party's decision to rely on a certificate may be assessed by the Relying Party themselves or by an entity controlling or coordinating the way that the Relying Party or Relying Party applications use the certificate. In these cases, the Relying Party obligations are extended to the entity controlling or coordinating the use of the certificate.

A Relying Party shall:

a) Perform intended cryptographic operations using appropriate software and hardware;
b) Prior to relying on a certificate, check the status of the certificate against the appropriate and current CRL or the OCSP server of a Certificate Status Authority in accordance with the requirements stated in Section 4.9.6 or 4.9.10 as applicable.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

9.6.5.1 DESIGNATED ORGANIZATION REPRESENTATIONS AND WARRANTIES

Where Designated Organization applies to receive certificates for use by individuals, devices, applications or roles, the Designated Organization, in addition to the requirements of Section 9.6.3, shall also:

a) Assume full responsibility for the accuracy and completeness of all information submitted to the CA or RA, and for the use of any keys, certificates, hardware or software issued to its Subscribers by the CA;
b) Name and confirm the identity of one or more individuals authorized to act on its behalf ("Designated Responsible Individual(s)");
c) Through the Designated Responsible Individual(s), verify and communicate to the CA or an RA, the identity and credentials of individuals who are to hold certificates either for their own individual use or for use with devices, applications or organizational roles within the Designated Organization;
d) Certify that all information to be contained in such certificates and any request for CA services is accurate and complete;
e) Ensure that no one other than the Subscriber will have access to the private signature keys for which they are responsible;
f) Ensure that all activation data associated with the Personal Security Environments (PSEs) of such certificates remains confidential;
g) With respect to certificates for devices, applications or roles, ensure that only one individual is responsible for such certificate for any given period of time;
h) Notify the CA or an RA if the Designated Organization’s relationship with an LRA has changed such that the certificate should be revoked or updated, or if there is any change in the LRA’s information or authorization to act on behalf of the Designated Organization;
i) Document, hold and produce upon request records of Subscriber status and authorization for verification purposes, said records linking a specific individual to an assigned certificate throughout the period that the certificate is so assigned to that Subscriber; and
j) Ensure that Subscribers:
    i. Use or rely on keys or certificates only for purposes permitted by this Certificate Policy and any other agreements or arrangements the Designated Organization may have with the CRA or CBSA;
    ii. Perform intended cryptographic operations using appropriate software and hardware as approved by the TBS, CIOB;
    iii. Protect the private keys, passwords and key tokens (if applicable) entrusted to them in such manner as set out in this Certificate Policy or as directed and take all reasonable measures to prevent their loss, disclosure, modification or unauthorized use; and
    iv. Immediately notify the CA in such manner as specified by the CA in the event of the compromise or suspected compromise of the private keys associated with the certificate they hold.

A Designated Organization shall certify to the Application Responsible Owner that it has taken appropriate measures to:

a) Apply on a regular basis and keep up-to-date anti-virus mechanisms;
b) Implement a “security patches and software updates” policy;

c) Maintain firewall services to protect their IT environment, specifically opening only those ports required for business purposes and having a rules system where anything not specifically permitted, is denied;
d) Ensure that both the organization's IT environment and users of certificates issued under the CP are subject to corporate security policies;
e) Maintain configuration management for the client environment to minimize vulnerabilities;
f) Implement a password policy under which, at a minimum,
    i) vendor-supplied defaults for system passwords are changed immediately;
    ii) vendor-supplied passwords are not used;
    iii) client workstations, where feasible, have password protected user accounts; and
    iv) passwords, where feasible, are no shorter than 8 characters with a combination of uppercase and lowercase letters, numbers and special characters.

9.6.5.2 APPLICATION RESPONSIBLE OWNER (ARO) REPRESENTATIONS AND WARRANTIES

The CA shall issue certificates for applications where the ARO has certified to the CA that the application meets all the requirements of the applicable laws and policies of Canada.

The CA shall issue certificates for Programs where the ARO has certified to the CA that appropriate measures have been taken to ensure that:

a) The integrity of the Program application is maintained throughout its lifecycle;
b) The Program software is developed using a structured design methodology;
c) Fail secure mechanisms are implemented in applications;
d) Program Applications:
    i. Satisfy applicable Government of Canada privacy requirements;
    ii. Have been certified and accredited in accordance with government security requirements;
    iii. Advise users of security vulnerabilities and fixes;
    iv. Provide explicit notice of the action to perform a digital signing operation; and;
    v. Perform certificate status checking as stipulated in sections 4.9.6 and 4.9.10.
e) A Threat and Risk Assessment (TRA) that complies with the *Policy on Government Security* (Reference Q) has been completed;
f) A Privacy Impact Assessment (PIA) that complies with the *Policy on Privacy Protection* (Reference V) has been completed if required; and
g) The ARO has assessed and considered issues of potential liability arising out of the provision of this service on-line and the advisability of establishing limits on liability, and has taken steps to ensure that users of the service will be given effective notice of any such limitations.

9.7 DISCLAIMERS OF WARRANTIES

The Government of Canada, its employees, servants or agents, makes no representations, warranties or conditions express or implied, other than as expressly stated in this Certificate Policy or in any other document authorized for that purpose by the Government of Canada.

No joint venture, partnership, trust, agency or fiduciary relationship is established or deemed to be established between the Government of Canada and individuals, organizations or any others using certificates issued by the CA or by a CA cross-certified with it.

9.8 LIMITATIONS OF LIABILITY

The Government of Canada disclaims all liability of any kind whatsoever, including arising from tort, contract or any other form of claim in relation to the use, delivery, license or reliance upon certificates issued under this Certificate Policy or associated public/private key pairs for any use other than in accordance with this Certificate Policy and any other agreements or written arrangements.

The Government of Canada 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 Programs.

The Government of Canada disclaims all liability, resulting from any action or inaction on the part of a Designated Organization, of any kind arising from tort, contract or any other form of claim in relation to the use, delivery, license or reliance upon certificates where a Designated Organization directs the issuance of certificates to Subscribers.

Departments may establish their own liability limits based upon individual Threat Risk Assessments.

System maintenance or factors outside the control of the CA may affect the availability of services provided by the CA. The Government of Canada disclaims all liability of any kind whatsoever for matters outside of its control including the availability of the Internet, or telecommunications or other infrastructure systems. Any use of the term “assurance” in this document is not a representation or warranty as to such availability of services.

The CA disclaims all liability of any kind whatsoever with respect to applications using certificates issued by it. With respect to the use of Program applications, Subscribers are advised to consult departments or agencies using certificates issued under this CP to determine if they have established liability limits. Nothing in this Certificate Policy creates, alters or eliminates any other obligation, responsibility, or liability that may be imposed on or assumed by a department or agency that makes use of the services provided by the CA for their respective Programs. The responsibility to establish any liability limits of the Government of Canada in connection with a Program remains with a Program Business Manager (PBM).

The rights, privileges and obligations, including limitations on liability, of a Relying Party who is a Subscriber of another CA may be addressed in an agreement between that Subscriber and that other CA.

The disclaimers and limitations of liability in these CPs are subject to any agreement or arrangement that may be entered into by the Crown in right of Canada that provides otherwise.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CP becomes effective when approved by CRA PKI PMA. This CP has no specified term.

9.10.2 TERMINATION

Termination of this CP is at the discretion of CRA PKI PMA.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

No stipulation.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

CRA PKI PMA may amend this Certificate Policy, or any part thereof, at any time at its discretion.

Departments may adopt this Certificate Policy for their own purposes.

Prior to any amendment of this Certificate Policy, CRA PKI PMA shall provide notice of any proposed change in writing to the Canadian Federal PKI Bridge (CFPB) as well as all CAs that are directly cross-certified with the CFPB and may specify a comment period in any such notice.

When a certificate is created the policy document with version and sub-version will be included in the certificate.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

The CA shall:

a) Provide Subscribers and Relying Parties with the URL of a Web Site;
b) Publish its CP, digitally signed by an authorized representative of the CA, on the web site mentioned above;
c) Inform, or cause Departments to inform, Subscribers and Relying Parties of any changes concerning their rights, privileges and obligations with respect to certificates; and
d) Provide in its discretion to relevant parties, on such terms and conditions it deems appropriate, all or part of the CPS, for the purposes of any audit, inspection, accreditation or cross-certification.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute related to key and certificate management between the Government of Canada and an organization or individual outside of the Government of Canada should be resolved using an appropriate dispute settlement mechanism. A dispute should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved using an independent mediator acceptable to the parties to the dispute. A dispute not settled by mediation should be resolved through arbitration in accordance with the *Commercial Arbitration Act (Reference W).*

A dispute related to key and certificate management between departments should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved as per the dispute resolution provisions contained within the Cross-Certification Memorandum of Understanding.

A dispute related to key and certificate management within a Department is to be resolved by the appropriate Departmental authority in conjunction with the Issuing CA.

The CA shall ensure that appropriate dispute resolution processes are included in any agreement or arrangement that it enters into, or any terms and conditions of use it establishes.

9.14 GOVERNING LAW

The laws of Canada and applicable provincial and territorial laws, exclusive of their conflicts-of-laws principles, govern the enforceability, construction, interpretation and validity of this Certificate Policy.

Any agreement the CA enters into is to be governed by the laws of Canada and applicable provincial and territorial laws, exclusive of their conflicts-of-laws principles, concerning enforceability, construction, interpretation and validity of this Certificate Policy.

9.15 COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this policy are required to comply with applicable Canadian acts, legislation or regulations.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

No stipulation.

9.16.3 SEVERABILITY

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.

9.16.4 ENFORCEMENT (ATTORNEY’S FEES AND WAIVER OF RIGHTS)

No stipulation.

9.16.5 FORCE MAJEURE

No stipulation.

9.17 OTHER PROVISIONS

No stipulation

APPENDIX 1 - REFERENCES

Reference A Financial Administration Act
http://laws-lois.justice.gc.ca/eng/acts/f-11/FullText.html

Reference B RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
http://www.ietf.org/rfc/rfc3647.txt

Reference C Standard on Identity and Credential Assurance
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776

Reference D Guideline on Defining Authentication Requirements
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262

Reference E ITU X.501 (10/2012) – Information Technology – Open Systems Interconnect – The Directory Models

Reference F ITU X.520 (10/2012) – Information Technology – Open Systems Interconnection – The Directory: Selected attribute types

Reference G ITU X.509 (10/2012) – Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Reference H ISO/IEC 29115:2013 - Information technology -- Security techniques -- Entity authentication assurance framework

Reference I ITSP.30.031 V2 - User Authentication Guidance for Information Technology Systems
https://www.cse-cst.gc.ca/en/publication/itsp.030.031v2

Reference J NIST 800-63-2 - Electronic Authentication Guideline

Reference K Guideline on the Management of Public Key Infrastructure in the Government of Canada
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=20008

Reference L ITSG-22 Baseline Security Requirements for Network Security Zones
http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg22-eng.html

Reference M Operational Security Standard on Physical Security
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12329

Reference N PKI X.509 Certificate and CRL Fields and Extensions (RFC 5280),
https://tools.ietf.org/html/rfc5280

Reference O Directive on Departmental Security Management
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=HTML.

Reference P Security Equipment Guide
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm

Reference Q Policy on Government Security
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text

Reference R Library and Archives of Canada Act
http://laws-lois.justice.gc.ca/eng/acts/L-7.7/

Reference S IETF RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Version 1
http://www.ietf.org/rfc/rfc2560.txt

Reference T Privacy Act
http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html

Reference U Access to Information Act
http://laws-lois.justice.gc.ca/eng/acts/a-1/

Reference V Policy on Privacy Protection
http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

Reference W Commercial Arbitration Act
http://laws-lois.justice.gc.ca/eng/acts/C-34.6/page-1.html

Reference X Conflict of Interest and Post-Employment Code for the Public Service
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25178

Reference Y Operational Security Standard - Business Continuity Planning (BCP) Program
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12324

Reference Z Cryptographic Algorithms for UNCLASSFIED, PROTECTED A, and PROTECTED B Information https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111