



Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Public Key Infrastructure Certificate Policy

External Reporting - Confidentiality
External Reporting - Digital Signature

May 2008

TABLE OF CONTENTS

1. INTRODUCTION.....	3		
1.1 OVERVIEW	3	3.1.3	Anonymity of Subscribers and Designated Certificate Holders.....20
1.2 POLICY IDENTIFICATION	3	3.1.4	Rules for Interpreting Various Name Forms.....20
1.3 PKI PARTICIPANTS.....	4	3.1.5	Uniqueness of Names.....20
1.3.1 Certification Authority.....	4	3.1.6	Recognition, Authentication and Roles of Trademarks.....20
1.3.2 Registration Authorities	4	3.2	INITIAL IDENTITY VALIDATION.....21
1.3.3 Subscribers.....	5	3.2.1	Method to Prove Possession of Private Key...21
1.3.4 Client Organizations	5	3.2.2	Authentication of an Organization Identity.....21
1.3.5 Relying Parties.....	5	3.2.3	Authentication of an Individual Identity.....21
1.3.6 Other Participants	5	3.3	IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS.....22
1.4 CERTIFICATE USAGE	6	3.3.1	Identification and Authentication for Routine Re-key.....22
1.4.1 Appropriate Certificate Uses.....	6	3.3.2	Identification and Authentication for Re-key after Revocation.....22
1.4.2 Prohibited Certificate Uses.....	6	3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....22
1.5 POLICY ADMINISTRATION	6	3.5	IDENTIFICATION AND AUTHENTICATION FOR RECOVERY REQUEST.....22
1.5.1 Organization Responsible for these Certificate Policies	6	4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	24
1.5.2 Contact Information	6	4.1	APPLICATION FOR A CERTIFICATE.....24
1.5.3 Notice and Publication.....	7	4.2	CERTIFICATE ISSUANCE.....24
1.5.4 Certificate Policy Amendment	7	4.3	CERTIFICATE ACCEPTANCE.....24
1.5.5 Certification Practice Statement Approval.....	7	4.4	CERTIFICATE REVOCATION OR SUSPENSION.....24
1.6 DEFINITIONS AND ACRONYMS	7	4.4.1	Circumstances for Revocation.....25
1.6.1 General Definitions.....	7	4.4.2	Who Can Request Revocation.....25
1.6.2 Acronyms.....	11	4.4.3	Procedure for Revocation Request.....25
2. GENERAL, LEGAL AND BUSINESS PROVISIONS.....	13	4.4.4	Revocation Request Grace Period.....25
2.1 REPRESENTATIONS AND WARRANTIES.....	13	4.4.5	Circumstances for Suspension.....25
2.1.1 CA Representations and Warranties.....	13	4.4.6	Who can Request Suspension.....26
2.1.2 RA Representations and Warranties.....	14	4.4.7	Procedure for Suspension Request.....26
2.1.3 Subscriber Representations and Warranties..	15	4.4.8	Limits on Suspension Period.....26
2.1.4 Client Organization Representations and Warranties	15	4.4.9	CRL Issuance Frequency.....26
2.1.5 Relying Party Representations and Warranties16		4.4.10	CRL Checking Requirements.....26
2.1.6 Repository Manager Representations and Warranties	16	5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS.....	27
2.2 DISCLAIMERS OF WARRANTIES	17	5.1	PHYSICAL CONTROLS.....27
2.3 LIMITATIONS OF LIABILITY.....	17	5.1.1	Site Location and Construction.....27
2.4 CROSS-CERTIFICATION AND RECOGNITION.....	17	5.1.2	Physical Access.....27
2.5 PRIVACY AND DATA PROTECTION	17	5.1.3	Power and Air Conditioning.....27
2.5.1 Sensitivity of Types of Private Information	18	5.1.4	Water Exposures.....27
2.5.2 Permitted Collection of Private Information	18	5.1.5	Fire Prevention and Protection.....27
2.5.3 Permitted Use of Private Information.....	18	5.1.6	Media Storage.....27
2.5.4 Permitted Distribution of Personal Information18		5.1.7	Waste Disposal.....27
2.5.5 Opportunity of Owner to Correct Private Information.....	18	5.1.8	Off-site Backup.....28
2.5.6 Release of Private Information to Law Enforcement Officials.....	18	5.2	PROCEDURAL CONTROLS.....28
2.5.7 Release of Private Information in Legal Proceedings.....	19	5.2.1	Trusted Roles.....28
2.6 FINANCIAL RESPONSIBILITY	19	5.2.2	Number of Persons Required per Task.....28
2.7 INTERPRETATION AND ENFORCEMENT	19	5.2.3	Identification and Authentication for Each Role28
2.7.1 Governing Law.....	19	5.3	PERSONNEL CONTROLS.....29
2.7.2 Dispute Resolution Procedures	19	5.3.1	Qualifications, Experience, and Clearance Requirements.....29
2.8 FEES	19	5.3.2	Background Check Procedures.....29
2.9 INTELLECTUAL PROPERTY RIGHTS	19	5.3.3	Training Requirements.....29
2.10 CRYPTOGRAPHIC PRODUCTS REGULATION	19	5.3.4	Retraining Frequency and Requirements.....29
3. IDENTIFICATION AND AUTHENTICATION	20	5.3.5	Job Rotation Frequency and Sequence.....29
3.1 NAMING	20	5.3.6	Sanctions for Unauthorized Actions.....30
3.1.1 Types of Names.....	20	5.3.7	Independent Contractor Requirements.....30
3.1.2 Need for Names to be Meaningful.....	20		

5.3.8	Documentation Supplied to Personnel	30
5.4	AUDIT LOGGING PROCEDURES	30
5.4.1	Types of Events Recorded	30
5.4.2	Frequency of Audit Log Processing.....	31
5.4.3	Retention Period for Audit Log	31
5.4.4	Protection of Audit Log	31
5.4.5	Audit Log Back-up Procedures	31
5.4.6	Audit Collection System.....	31
5.4.7	Notification of Event Causing Subject	31
5.4.8	Vulnerability Assessments.....	32
5.5	RECORDS ARCHIVAL	32
5.6	KEY CHANGEOVER.....	33
5.7	COMPROMISE AND DISASTER RECOVERY	33
5.7.1	Computing Resources, Software and/or Data Corrupted.....	33
5.7.2	CA Public Certificate Revocation.....	33
5.7.3	CA Key Compromise	33
5.7.4	Business Continuity Capabilities After a Disaster.....	34
5.8	CA TERMINATION/CHANGE IN OPERATIONS	34
6.	TECHNICAL SECURITY CONTROLS ..	35
6.1	KEY PAIR GENERATION AND INSTALLATION	35
6.1.1	Key Pair Generation	35
6.1.2	Private Key Delivery to Subscriber/Designated Certificate Holder	35
6.1.3	Public Key Delivery to Certificate Issuer.....	36
6.1.4	CA Public Key Delivery to Subscribers.....	36
6.1.5	Key Sizes.....	36
6.1.6	Public Key Parameters Generation and Quality Checking.....	36
6.1.7	Key Usage Purposes (as per x509v3 field)	36
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	36
6.2.1	Cryptographic Module Standards and Controls	36
6.2.2	Private Key Multi-person Control	37
6.2.3	Private Key Escrow.....	37
6.2.4	Private Key Back-up	37
6.2.5	Private Key Archival.....	37
6.2.6	Private Key Transfer Into or From a Cryptographic Module.....	38
6.2.7	Private Key Storage on Cryptographic Module	38
6.2.8	Method of Activating Private Key	38
6.2.9	Method of Deactivating Private Key	38
6.2.10	Method of Destroying Private Key	38
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT .	38
6.3.1	Public Key Archival.....	38
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	38
6.3.3	CA Key Storage, Backup and Recovery.....	39
6.3.4	Key Recovery by Subscriber or Designated Certificate Holder	39
6.4	ACTIVATION DATA	39
6.4.1	Activation Data Generation and Installation ...	39
6.4.2	Activation Data Protection	40
6.4.3	Other Aspects of Activation Data.....	40
6.5	COMPUTER SECURITY CONTROLS	40
6.5.1	Specific Computer Security Technical Requirements	40
6.5.2	Computer Security Rating.....	40
6.6	LIFE CYCLE TECHNICAL CONTROLS	41
6.6.1	System Development Controls	41
6.6.2	Security Management Controls	41
6.7	NETWORK SECURITY CONTROLS	41
6.8	TIME-STAMPING	41

7. CERTIFICATE AND CRL PROFILES.... 42

7.1	CERTIFICATE PROFILE.....	42
7.1.1	Version Number	42
7.1.2	Certificate Extensions	42
7.1.3	Algorithm Object Identifiers	43
7.1.4	Name Forms	43
7.1.5	Name Constraints	43
7.1.6	Certificate Policy Object Identifier	43
7.1.7	Usage of Policy Constraints Extension	43
7.1.8	Policy Qualifiers Syntax and Semantics.....	43
7.1.9	Processing Semantics for Critical Certificate Extensions.....	44
7.2	CRL PROFILE	44
7.2.1	Version Number	44
7.2.2	CRL and CRL Entry Extensions.....	44

8. COMPLIANCE INSPECTION AND OTHER ASSESSMENTS 45

8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	45
8.2	IDENTITY AND QUALIFICATIONS OF ASSESSOR .	45
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	45
8.4	TOPICS COVERED BY ASSESSMENT.....	45
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .	46
8.6	COMMUNICATION OF RESULTS	46

1. INTRODUCTION

1.1 Overview

This document defines the following Certificate Policies (CPs) for the issuance of Digital Signature and Confidentiality certificates for use for electronic reporting to FINTRAC:

- External Reporting Digital Signature Certificate Policy
- External Reporting Confidentiality Certificate Policy

Certificates issued under these Certificate Policies are to be used exclusively to deal with FINTRAC and are “enterprise certificates”. Enterprise certificates securely bind the holder of a certificate to its public keys and are managed within a Public Key Infrastructure (PKI).

Standard commercial browsers support the use of “Web certificates” but not enterprise certificates. The Certification Authority (CA) operating under these Certificate Policies does not support Web certificates.

The External Reporting digital signature policy is for the management and use of certificates containing public keys used for authentication and data integrity.

The External Reporting confidentiality policy is for the management and use of certificates containing public keys used for encryption key establishment, including key transfer. The certificates issued under this policy are suitable for protecting information.

Unless used in conjunction with other security mechanisms, these certificates are not to be used for the protection of information that, if compromised could cause extremely grave injury outside of the national interest or for classified information. These certificates are not to be used where prohibited by law or with applications requiring fail-safe performance.

FINTRAC disclaims all liability of any kind arising from tort, contract or any other form of claim in relation to the use, delivery, license or reliance upon certificates issued under these Certificate Policies or associated public/private key pairs for any use other than in accordance with these Certificate Policies and any other related agreements.

System maintenance or factors outside the control of the CA may affect the availability of services provided by the CA. FINTRAC disclaims all liability of any kind for matters outside of its control including the availability or working 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.

1.2 Policy Identification

DIGITAL SIGNATURE	CONFIDENTIALITY
The name of this policy is FINTRAC External Reporting PKI Digital Signature Certificate Policy.	The name of this policy is FINTRAC External Reporting PKI Confidentiality Certificate Policy.
The alphanumeric and numeric object identifier (OID) for this policy is: 2.16.124.101.1.275.2	The alphanumeric and numeric object identifier (OID) for this policy is: 2.16.124.101.1.275.1

1.3 PKI Participants

These Certificate Policies support a PKI community as defined in the following sub-sections.

1.3.1 Certification Authority

All references to the Certification Authority (CA) refer to the FINTRAC CA unless stated otherwise.

The CA may retain the services of any third party to perform its assigned responsibilities under these Certificate Policies.

The CA is accountable to the FINTRAC Policy Management Authority for the:

- a) Application of certificate policies selected or defined by the FINTRAC Policy Management Authority;
- b) Development of a Certification Practice Statement (CPS), in accordance with these Certificate Policies, to document the CA's compliance with the certificate policies and other requirements;
- c) Maintenance of the CPS to ensure that it is updated as required; and
- d) Supervision of CA personnel performing CA functions in accordance with the CPS.

With respect to the actual operation of CA servers, there are significant roles that should be noted:

- 1) A PKI Master User who is responsible for the configuration and maintenance of hardware and software for the CA system; commencement and cessation of CA services; and the initial creation of accounts for PKI Officers.
- 2) A PKI Officer who is responsible for the management of PKI Administrators as well as other PKI Officers and the configuration of CA security policies.
- 3) A PKI Administrator who is responsible for the management of the Subscriber initialization process; the creation, renewal or revocation of certificates and the distribution of tokens (where applicable).

CA personnel shall not audit their own activities.

Associated with the CA is a PKI Help Desk, which is responsible for the provision of assistance to Subscribers and Designated Certificate Holders with respect to certificate issuance, maintenance or revocation.

1.3.2 Registration Authorities

A Registration Authority (RA) is an individual or organization, acting on behalf of the CA, responsible for verifying the identity of a Subscriber or, in the case of a Client Organization, a Designated Certificate Holder. If required, the RA may verify a Designated Certificate Holder's authority to act on behalf of a Client Organization. While the RA initiates the process to cause the CA to issue certificates, it does not sign or issue certificates. The RA may employ a system where the identification process can be done automatically through shared secrets and may perform such other duties as requested of it by the CA.

1.3.3 Subscribers

The following may be Subscribers of the CA:

- 1) Individuals acting in their own capacity;
- 2) Organizations outside of FINTRAC in any form recognized by law.

Subscriber eligibility for a certificate is at the sole discretion of the CA.

Certificates governed by these Certificate Policies may be issued to FINTRAC employees, roles, devices or applications to facilitate program delivery but they are not Subscribers for the purposes of these Certificate Policies and other instruments will govern their rights, privileges and obligations.

1.3.4 Client Organizations

As noted, one form of Subscriber is an organization outside of FINTRAC. These organizations may wish to obtain certificates to be used by their employees or, from time to time, others as appropriate that are authorized to act in a capacity on behalf of the organization. These individuals are identified as Designated Certificate Holders for the purpose of having custody of certificates to be issued for use by individuals, devices, roles or applications associated with a Client Organization.

Certificates for use within Client Organizations shall only be issued upon request by an individual identified by the organization as its Client Responsible Individual (CRI) who is authorized to make such a request.

Client Organization eligibility for certificates is at the sole discretion of the CA.

1.3.5 Relying Parties

A Relying Party is either:

- a) A Subscriber of the FINTRAC CA;
- b) An individual who is a FINTRAC employee or authorized contractor; or
- c) A device or application under the control of FINTRAC

that uses a certificate issued under these Certificate Policies and signed by the CA to authenticate a digital signature or to encrypt communications to a certificate holder.

Individuals or organizations, other than those listed above are not entitled to rely upon certificates issued by the CA and, any such reliance is done at their own risk. FINTRAC disclaims any and all liability that may arise out of any such reliance.

1.3.6 Other Participants

FINTRAC Policy Management Authority

The FINTRAC Policy Management Authority is an internal committee consisting of senior management within FINTRAC that is responsible for:

- a) Approving the FINTRAC's CA's Certificate Policies;
- b) Approving the FINTRAC's CA's Certification Practice Statement; and
- c) Providing policy direction to the FINTRAC CA.

Repository Manager

The Repository Manager is an individual or organization responsible for maintaining a repository holding relevant information such as certificates and Certificate Revocation Lists (CRL).

The CA will have at least one certificate and CRL repository associated with it.

The CA may, but need not, perform this function. 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 and directory chaining.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

DIGITAL SIGNATURE	CONFIDENTIALITY
This policy is suitable for the integrity and authentication of transactions or communications.	This policy is suitable for protecting information.

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA shall not be used for:

- 1) Any application requiring fail-safe performance;
- 2) Transactions where applicable law prohibits the use of digital signatures for such transactions or where otherwise prohibited by law; or
- 3) Unless supported by other appropriate security mechanisms, the protection of:
 - i) Information that, if compromised, could cause extremely grave injury outside the national interest; or
 - ii) Classified information.

1.5 Policy Administration

1.5.1 Organization Responsible for these Certificate Policies

The FINTRAC Policy Management Authority (FINTRAC PMA) is responsible for these Certificate Policies.

1.5.2 Contact Information

Chairperson, FINTRAC Policy Management Authority
FINTRAC
234 Laurier Avenue West, 24th floor
Ottawa, Ontario, Canada
K1P 1H7
Fax: (613) 943-7931
Email: pki-icp@fintrac-canafe.gc.ca

1.5.3 Notice and Publication

The CA shall:

- a) Provide Subscribers, Client Organizations, Designated Certificate Holders and Relying Parties with the URL of its Web Site;
- b) Publish its CP on its Web site;
- c) Inform Subscribers, Designated Certificate Holders and Relying Parties of any changes concerning their rights, privileges and obligations with respect to certificates;
- 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, or accreditation.

1.5.4 Certificate Policy Amendment

The FINTRAC PMA may amend these Certificate Policies, or any part thereof, at any time at its discretion.

1.5.5 Certification Practice Statement Approval

Following a determination that the CPS sets out in a satisfactory manner how the CA will implement the requirements of these Certificate Policies, the FINTRAC PMA shall approve the Certification Practice Statement (CPS) associated with these Certificate Policies and any amendments thereto.

1.6 Definitions and Acronyms

1.6.1 General Definitions

Activation data	Private data, other than keys, required to access Personal Security Environments that need to be protected (e.g., password).
Authority Revocation List	A list of revoked CA certificates. An ARL is a Certificate Revocation List for CA cross-certificates or self-signed certificates.
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 or Designated Certificate Holder, 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.

<p>Certification Authority</p>	<p>An Entity trusted by one or more End Entities to issue and manage X.509 public key certificates and CRLs.</p> <p>The CA is accountable to the Policy Management Authority for the:</p> <ul style="list-style-type: none"> a) Application of certificate policies selected or defined by the Policy Management Authority; b) Development of a Certification Practice Statement (CPS), in accordance with these Certificate Policies to document the CA's compliance with certificate policies and other requirements; c) Maintenance of the CPS to ensure that it is updated as required; and d) Supervision of CA personnel performing CA functions in accordance with the CPS.
<p>Certification Authority Software</p>	<p>Software that manages the CA signing key, the life cycle of certificates and CRLs as well as key pairs of end-entities.</p>
<p>Certification Validation Chain</p>	<p>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.</p> <p>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.</p>
<p>Client Organization</p>	<p>An organization that is a client or Reporting Entity of FINTRAC.</p>
<p>Client Responsible Individual</p>	<p>An individual within a Client Organization authorized by it to represent and to act on behalf of the organization for the purpose of applying for the issuance of certificates. The Client Responsible Individual is typically responsible for:</p> <ul style="list-style-type: none"> a) Verification and confirmation of the identity and credentials of Designated Certificate Holders within a Client Organization; b) Communication to the CA of any change in the Client Organization's relationship with, or information provided about, a Designated Certificate Holder that would result in certificate termination or update.
<p>Configuration Management</p>	<p>A process to identify and define critical items in the system and to control any change of these items throughout their lifecycle.</p>
<p>Controlled Environment</p>	<p>A combination of hardware and software products, configuration management, policy and procedures to manage Subscriber or Designated Certificate Holder environments controlled by a Program Business Manager and/or the Client Organization. If a Client Organization primarily controls the environment, the business relationship between the Program and the Client Organization may include security obligations in any Program-related agreements in order to minimize security risks.</p>
<p>Cross-certificate</p>	<p>A certificate issued by a Certification Authority to establish a trust relationship between it and another Certification Authority.</p>

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.
Department or Agency	Those departments listed in Schedule I, Schedule I.1 and Schedule II of the Financial Administration Act (FAA) and (a) Any commission under the Inquiries Act that is designated by order of the Governor in Council as a department for the purposes of the FAA; (b) The Canadian Forces; and (c) Those agencies or crown corporations that have entered into agreements or arrangements with the Treasury Board Secretariat to adopt the requirements of this certificate policy and apply them to their organizations.
Designated Certificate Holder	An individual within a Client Organization who is designated as the holder of a certificate issued to an individual, role, device or application within a Client Organization.
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: a) The transformation was created using the key that corresponds to the signer's key; and b) The data has been altered since the transformation was made.
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 Designated Certificate Holder, a Relying Party, or a device, a role or an application using a certificate assigned to a Designated Certificate Holder.
Enrolment	A process by which an individual or an organization registers to receive services from or make transactions with FINTRAC.
Enterprise Certificate	A certificate issued by a CA for use by individuals, organizations, roles, devices or applications. These certificates are fully managed within a PKI and may be subject to: a) Automatic revocation checking; b) Transparent credential update; and c) Dynamic and transparent security policy update. An Enterprise certificate securely binds the owner of the certificate to its public keys. Standard commercial browsers do not support use of Enterprise certificates.
Entity	Any autonomous element within the PKI. This may be a CA, an RA or an End-Entity.
Fail Safe	The structuring of programs and/or processing systems to maintain safety and/or to accomplish their assigned missions when a hardware or software failure is detected in a program or system.

Fail Secure	The structuring of programs and/or processing systems in a manner that security vulnerabilities are not introduced when a hardware or software failure is detected in a program or system.
FINTRAC Policy Management Authority	The FINTRAC Policy Management Authority is an internal committee consisting of senior management within FINTRAC that is responsible for: <ul style="list-style-type: none"> a) Approving FINTRAC's CA's Certificate Policies; b) Approving FINTRAC's CA's Certification Practice Statement; and c) Providing policy direction to the FINTRAC CA.
Individual	A single, natural person as distinguished from a group or class or any type of organization.
Initialization data	Codes or other data used by a Subscriber or Designated Certificate Holder to generate a private digital signature key and obtain public key certificates from the CA (e.g. reference number and authentication code).
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.
Organization	An agency, corporation, partnership, trust, joint venture or other association. If recognized as such, an organization may include a sole proprietorship.
Personal Security Environment	A secure storage area containing information such as private keys and related certificates. The storage area is encrypted and protected using cryptography. The form of storage may vary from files to tamper-resistant cryptographic tokens.
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 who is responsible for the management of the Subscriber initialization process; the creation, renewal or revocation of certificates and the distribution of tokens (where applicable).
PKI Master User	An individual who is responsible for the configuration and maintenance of hardware and software for the CA system; commencement and cessation of CA services and the initial creation of accounts for PKI Officers.
PKI Officer	An individual who is responsible for the management of PKI Administrators as well as other PKI Officers and the configuration of CA security policies.
Registration Authority	A person or organization that is responsible for the identification and authentication of Subscribers and other End Entities before certificate issuance, but does not sign or issue the certificates. An RA may be asked to perform certain tasks on behalf of the CA.

Relying Party	<p>An Entity that is:</p> <ul style="list-style-type: none"> a) A Subscriber of the FINTRAC CA; b) An individual who is a FINTRAC employee or authorized contractor; or c) A device or application under the control of FINTRAC <p>that uses a certificate, issued under these Certificate Policies and signed by the CA, to authenticate a digital signature or to encrypt communications to a certificate holder.</p>
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 organization responsible for maintaining a repository holding relevant information such as certificates and Certificate Revocation Lists.
Security Zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. A Security Zone should be monitored 24 hours a day 7 days a week by security staff, other personnel or electronic means.
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 or Designated Certificate Holders wish to use their keys, they access their profile using a specific user ID and password known only to them; retrieve the encrypted profile through a SSL tunnel and, following its use, the local copy of the profile is destroyed. At no time is the profile outside the exclusive control of the Subscriber or Designated Certificate Holder.
Subscriber	An individual or organization whose public key certificates are signed by the CA operating under these Certificate Policies.
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.

1.6.2 Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CCF	Canadian Central Facility
CO	Client Organization
CP	Certificate Policy
CPS	Certification Practice Statement
CRI	Client Responsible Individual
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DCH	Designated Certificate Holder
DES	Data Encryption Standard
DN	Distinguished Name
FIPS	Federal Information Processing Standards
GoC	Government of Canada
GOL	Government of Canada On-Line

I&A	Identification and Authentication
ITU	International Telecommunications Union
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PBM	Program Business Manager
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PSE	Personal Security Environment
RA	Registration Authority
RDN	Relative Distinguished Name
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm -1
SSL	Secure Sockets Layer
TRA	Threat and Risk Assessment
URL	Uniform Resource Locator

2. GENERAL, LEGAL AND BUSINESS PROVISIONS

2.1 Representations and Warranties

2.1.1 CA Representations and Warranties

DIGITAL SIGNATURE	CONFIDENTIALITY
<p>The CA is responsible for:</p> <ul style="list-style-type: none"> a) The creation and signing of certificates binding Subscribers, Designated Certificate Holders, PKI personnel and (where permitted) other CAs with their public verification keys; and b) Promulgating certificate status through CRLs. <p>The CA may also generate End-Entity Digital Signature key pairs when using automated registration processes.</p>	<p>The CA is responsible for:</p> <ul style="list-style-type: none"> a) The creation and signing of certificates binding Subscribers, Designated Certificate Holders and PKI personnel with their public encryption keys; and b) Promulgating certificate status through CRLs. <p>The CA will also generate End-Entity Confidentiality key pairs if required to do so.</p>

The CA shall:

- 1) Operate for the purpose of issuing and managing certificates for Subscribers, Designated Certificate Holders, CA personnel, RAs and Repository Managers, as required, in accordance with these Certificate Policies, the applicable CPS, and applicable laws of Canada;
- 2) Prepare a CPS describing in detail all practices, procedures and requirements required to comply with these Certificate Policies;
- 3) Ensure that all RAs and Repository Managers acting on its behalf operate in accordance with these Certificate Policies and the applicable CPS;
- 4) Ensure that appropriate agreements outlining the respective rights, privileges and obligations of the parties are entered into with:
 - (a) Subscribers for certificates issued to them or assigned on their direction; and
 - (b) All others who are performing functions on behalf of the CA.
- 5) 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;
- 6) Endeavour to provide Subscribers, Client Responsible Individuals, 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;
- 7) Notify a Subscriber, a Client Responsible Individual or Designated Certificate Holder, as the case may be, when a certificate for their use is:
 - (a) Issued;
 - (b) Suspended; or
 - (c) Revoked.

- 8) Ensure that the initialization process is completed within a predetermined period as documented in the CPS;
- 9) Provide notice in certificates issued under these policies as to the address of the CRL;
- 10) Provide appropriate notice to all interested parties as to the CA's procedures concerning the expiration, suspension, revocation and renewal of certificates;
- 11) Make CRLs available to a Subscriber, Designated Certificate Holder or Relying Party as required under these Certificate Policies;
- 12) Use its certificate signing private key only to sign certificates and CRLs and for no other purpose;
- 13) Institute procedures to ensure CA personnel associated with PKI roles (e.g. PKI Master User; PKI 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; and
- 14) Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

Except as otherwise provided, 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 these Certificate Policies.

DIGITAL SIGNATURE	CONFIDENTIALITY
When required as a result of the technology used, the CA shall place Subscriber or Designated Certificate Holder private signature keys in Storage.	When required as a result of the technology used, the CA shall place Subscriber or Designated Certificate Holder private decryption keys in Storage.

2.1.2 RA Representations and Warranties

The RA shall:

- 1) Comply with applicable provisions of these Certificate Policies and CPS, and with the terms and conditions of any agreement or arrangement with the CA;
- 2) Inform applicants of the application process, including the process for the initialization of certificates;
- 3) 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 these Certificate Policies;
- 4) Inform Subscribers, Client Responsible Individuals or Designated Certificate Holders, as the case may be, 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;
- 5) Where the CA does not record the information, ensure, for audit purposes, that records of actions carried out in performance of RA duties are maintained.
- 6) Protect the RA's private keys as directed by the CA.

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

2.1.3 Subscriber Representations and Warranties

A Subscriber shall:

- 1) Ensure that information submitted to the CA or RA directly or on their behalf is complete and accurate;
- 2) Comply with the terms of the applicable Subscriber Agreement or other binding instrument satisfactory to the CA;
- 3) Use or rely on keys or certificates only for purposes permitted by these Certificate Policies and for no other purpose;
- 4) Perform intended cryptographic operations using appropriate software and hardware;
- 5) Protect their private keys, passwords and key tokens (if applicable) in such manner as set out in these Certificate Policies or as directed and take all reasonable measures to prevent their loss, disclosure, modification or unauthorized use;
- 6) 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;
- 7) 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);
- 8) With respect to the use outside of Canada of hardware or software containing cryptographic products or elements, verify that the:
 - i) Importation and/or use of such products is permitted within a particular country or jurisdiction; and
 - ii) Exportation of such products from Canada to another country or jurisdiction is permitted.

2.1.4 Client Organization Representations and Warranties

Where a Subscriber is an organization ("Client Organization") and applies to receive certificates for use by individuals, devices, applications or roles ("Designated Certificate Holders"), the Client Organization, in addition to the requirements of Section 2.1.3, shall also:

- 1) Assume full responsibility for the use of any keys, certificates, hardware or software issued to Designated Certificate Holders by the CA;
- 2) Name and confirm the identity of one or more individuals authorized to act on its behalf ("Client Responsible Individual(s)");
- 3) Through these Client 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 Client Organization;
- 4) Certify that all information to be contained in such certificates and any request for CA services will be accurate and complete;
- 5) Ensure that no one other than the Designated Certificate Holder will have access to the private signature keys for which they are responsible;
- 6) Ensure that all activation data associated with the Personal Security Environments (PSEs) of such certificates remains confidential;

- 7) 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;
- 8) Notify the CA or an RA if the Client Organization's relationship with a Designated Certificate Holder has changed such that the certificate should be revoked or updated, or if there is any change in the Designated Certificate Holder's information or authorization to act on behalf of the Client Organization with respect to reporting to FINTRAC;
- 9) Document, hold and produce upon request records of employee 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 Designated Certificate Holder;
- 10) Ensure that Designated Certificate Holders:
 - i) Use or rely on keys or certificates only for purposes permitted by these Certificate Policies;
 - ii) Perform intended cryptographic operations using appropriate software and hardware;
 - iii) Protect the private keys, passwords and key tokens (if applicable) entrusted to them in such manner as set out in these Certificate Policies 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.

The private keys of a Subscriber or Designated Certificate Holder must be stored securely in a Personal Security Environment (PSE).

A Client Organization should:

- a) Apply on a regular basis and keep up-to-date anti-virus mechanisms;
- b) Apply software updates to client workstations;
- c) Protect client workstations using firewall services;
- d) Maintain configuration management for the client environment to minimize vulnerabilities;
- e) Maintain a clear separation of duty between system administration, oversight activities (e.g., audits) and system users; and
- 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.

2.1.5 Relying Party Representations and Warranties

A Relying Party shall:

- 1) Perform intended cryptographic operations using appropriate software and hardware;
- 2) Prior to relying on a certificate:
 - i) Check the status of the certificate against the appropriate and current CRL in accordance with the requirements stated in Section 4.4.10 as applicable; and
 - ii) With respect to certificate validation using a CRL, validate the digital signature of the CA affixed to the CRL.

2.1.6 Repository Manager Representations and Warranties

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

- 1) Publish certificates and CRLs;
- 2) Inform Subscribers and Designated Certificate Holders of the location of any CRL server;
- 3) Publish the status of certificates through certificate revocation lists, or otherwise make information available within the timeframes specified in these Certificate Policies; and
- 4) Configure operating system and repository access controls so that only authorized CA personnel can write or modify the on-line version of the CP.

Where the CA does not operate a repository, the CA shall ensure, through contractual or other means, that the repository manager meets the foregoing requirements.

The CA may mandate repository access controls with respect to certificates, CRLs or on-line certificate status checking.

2.2 Disclaimers of Warranties

FINTRAC, its employees, servants or agents, makes no representations, warranties or conditions, express or implied, other than as expressly stated in these Certificate Policies or in any other document authorized for that purpose by FINTRAC.

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

2.3 Limitations of Liability

FINTRAC disclaims all liability of any kind arising from tort, contract or any other form of claim in relation to the use, delivery, license or reliance upon certificates issued under these Certificate Policies or associated public/private key pairs for any use other than in accordance with these Certificate Policies and any other related agreements.

FINTRAC 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.

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

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

2.4 Cross-certification and Recognition

Not applicable.

2.5 Privacy and Data Protection

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 collection, use and disclosure of private information as outlined in these Certificate Policies and in any related agreement.

2.5.1 Sensitivity of Types of Private Information

Private information is (1) identifiable information about an individual and (2) business confidential information from an organization. The sensitivity of private information held by FINTRAC, in connection with certificates issued under these Certificate Policies, is determined by reference to:

- 1) Applicable statutes and regulations, including but not limited to the *Privacy Act*, *Access to Information Act*, *Proceeds of Crime (Money Laundering) Terrorist Financing Act* and *National Archives of Canada Act*;
- 2) Applicable government security policies; and
- 3) Applicable government privacy policies.

Private information associated with the issuance of certificates under these Certificate Policies is considered particularly sensitive.

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

2.5.2 Permitted Collection of Private Information

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

2.5.3 Permitted Use of Private Information

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

2.5.4 Permitted Distribution of Personal Information

Subject to Sections 2.5.6 and 2.5.7 and the limitations and permissions imposed by the *Privacy Act* and other applicable statutes, regulations and policies, the CA and any RA may distribute private information only to FINTRAC personnel 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.

2.5.5 Opportunity of Owner to Correct Private Information

The owner of private information, or a Client 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.

2.5.6 Release of Private Information to Law Enforcement Officials

The CA or any RA shall only release private information, collected for the purpose of issuing and managing a certificate, to law enforcement officials upon receipt of (1) a judicial order; (2) the consent of the owner of the private information; or (3) where required or permitted pursuant to express statutory authority.

2.5.7 Release of Private Information in Legal Proceedings

The CA or any RA shall only release private information, collected for the purpose of issuing and managing a certificate, where requested to do so in connection with legal proceedings, upon receipt of (1) a judicial order; (2) the consent of the owner of the private information; or (3) where required or permitted pursuant to express statutory authority.

2.6 Financial Responsibility

In the event the CA contracts for the provision of any CA services, it shall ensure that any such service provider provides satisfactory evidence of financial responsibility and, if applicable, waives any legislative immunity.

2.7 Interpretation and Enforcement

2.7.1 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 these Certificate Policies.

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 these Certificate Policies.

2.7.2 Dispute Resolution Procedures

If there is any dispute between FINTRAC and the Subscriber, the parties will attempt to resolve the dispute amicably.

2.8 Fees

Not applicable.

2.9 Intellectual Property Rights

All right, title and interest in all intellectual property rights in or associated with these Certificate Policies, CRLs, ARLs, Distinguished Names, FINTRAC Service Arrangements, CA Public Keys and certificates as well as End Entity certificates (the "Materials"), including all modifications and enhancements thereof, are and shall remain the exclusive property of FINTRAC.

Subscribers, Designated Certificate Holders and Relying Parties may use the Materials only for the purposes of complying with these Certificate Policies. 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 FINTRAC 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.

2.10 Cryptographic Products Regulation

The export or import of software used to enable the provision of services offered by the CA may require the approval of appropriate government authorities. Anyone using the services provided by the CA shall comply with applicable export and import laws and regulations. The CA shall not be responsible for obtaining any necessary permission to enable such export or import of software or notifying users as to their existence or content.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

In accordance with the GoC X.509 Certificate and CRL Fields and Extensions Profile, each Entity:

- a) Must have a clearly distinguishable and unique x.501 Distinguished Name (DN) in the certificate subject name field; and
- b) May be assigned an alternative name via the SubjectAlternativeName field.

The DN must be in the form of a X.501 printable string and must not be blank.

3.1.2 Need for Names to be Meaningful

The Subject name in a certificate must be meaningful to the extent that FINTRAC has associated the certificate with an End Entity.

3.1.3 Anonymity of Subscribers and Designated Certificate Holders

The Relative Distinguished Name (RDN) may, but is not required to, visibly identify the legal or organizational name of an End Entity. Legal names, organizational names, alphanumeric identifiers or hashes of any of the foregoing may be used as a RDN.

Where a legal or organizational name is not used as an RDN of a certificate, the CA shall ensure that a record is retained of the name of a person who either holds a certificate or, in the case of a certificate for a device, role or application, is responsible for that certificate.

3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting name forms will be in accordance with the GoC Common Directory Schema, version 1.2 dated 30 November, 2000, as amended or revised.

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 of the CA. The SubjectUnique Identifiers field, as defined in the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, used to differentiate Subscribers with identical names, will not be supported.

The CA reserves the right to make decisions regarding Entity names in all assigned certificates. A party requesting a certificate may be required to demonstrate its right to use a particular name.

Where there is a dispute about a name in a repository not under its control, the CA shall ensure in its agreement with that repository that the repository has a name claim dispute resolution procedure.

3.1.6 Recognition, Authentication and Roles of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

DIGITAL SIGNATURE	CONFIDENTIALITY
Prior to the issuance of a verification certificate, the CA and End-Entity will confirm their respective identities in a secure manner.	Prior to the exchange of a private decryption key, the CA and End-Entity will confirm their respective identities in a secure manner.

3.2.2 Authentication of an Organization Identity

An organization must make an application to be a Subscriber through an individual acting 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 FINTRAC; or
- b) Copies of official documentation providing evidence of the existence of the organization.

The CA or RA must also verify the authority of the individual acting on behalf of the organization (i.e. Client Responsible Individual (CRI)).

The CA or RA shall ensure that a record is kept of the means by which the CRI has been established.

3.2.3 Authentication of an Individual Identity

Individuals in Their Own Capacity

A request by an individual seeking to be a Subscriber in his or her own capacity ("Prospective Subscriber") must be presented by the individual or by another individual authorized to act on behalf of the prospective Subscriber.

The identity of a Prospective Subscriber must be authenticated in any manner sufficient to satisfy the CA or an RA that the individual has the identity he or she claims to possess. The CA or an RA may authenticate the identity of a Prospective Subscriber using any one of the following means:

- a) Privately shared information if the identity of the individual has been previously established by FINTRAC for enrolment purposes;
- b) Two pieces of identification (notarized copies or originals), one of which must be government-issued identification containing a photograph; or
- c) Certified copies of two pieces of identification accompanied by the attestation of a person permitted to serve as a guarantor on a Canadian passport application that the person purporting to possess an identity is, to his or her knowledge, that person.

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, but is not obliged to keep a copy of the identification itself.

Individual as Designated Certificate Holder within a Client Organization

A request for an individual to be a Designated Certificate Holder acting on behalf of a Client Organization must be approved by a Client Responsible Individual (CRI) prior to its submission to the CA. The CRI must comply with the RA requirements stated in this Certificate Policy.

The identity of an individual must be authenticated in any manner sufficient to satisfy the CRI that the individual has the identity he or she claims to possess. A CRI must provide the following information to the CA:

- a) Identification information of the individual;
- b) Attestation to the fact that the identification and authentication was done; and
- c) Contact information to enable the CA or RA to communicate with the Subscriber and the CRI.

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 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.

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

A revocation request 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.

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

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

The CA must establish and make publicly available the process by which it addresses such a request and the means by which it will establish the validity of the request.

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

3.5 Identification and Authentication for Recovery Request

A recovery request 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.

The CA or an RA must authenticate all Subscriber requests for recovery of a PSE or a confidentiality private key. The authentication may be performed using privately shared information.

PSE or key recovery may be done through an automated process. The CA shall inform Subscribers and Designated Certificate Holders as to the process, whether automated or manual, by which they may make recovery requests and how such requests are to be authenticated.

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

Requests for PSE or key recovery must be recorded in a log.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Application for a Certificate

The CA shall:

- 1) State in the CPS all procedures and requirements with respect to applications for the issuance of certificates; and
- 2) Inform prospective certificate holders as to the information they must submit and the application process.

The CA shall ensure that terms and conditions of use govern each certificate it issues. Subscribers are to enter into an agreement or otherwise be subject to terms and conditions concerning their rights, privileges and obligations associated with certificates issued to them.

When submitting an application for a Designated Certificate Holder, a CRI shall refer to the name of the Client 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, to Designated Certificate Holders on behalf of the Client Organization.

An application for a certificate does not oblige the CA to issue a certificate. FINTRAC has the discretion to refuse to issue a certificate.

4.2 Certificate Issuance

The issuance of a certificate by the CA indicates a complete and final approval of the certificate application by the CA.

4.3 Certificate Acceptance

The use of the certificate by a Subscriber, Designated Certificate Holder or a role, device or application for which a certificate has been issued constitutes acceptance of a certificate and all obligations associated with its use.

4.4 Certificate Revocation or Suspension

DIGITAL SIGNATURE	CONFIDENTIALITY
In the event of the compromise of the CA signing key, the CA shall comply with the obligations described in section 5.7.3. In the event of the compromise, or suspected compromise, of any other Entity's signing key, the Entity must notify the CA immediately.	In the event of the compromise or suspected compromise of an Entity's decryption private key, the Entity must notify the CA immediately.

4.4.1 Circumstances for Revocation

Upon receipt of acceptable notice, the CA shall revoke a certificate in the following circumstances:

- 1) When any information in the certificate changes;
- 2) Upon the suspected or known compromise of the private key or the media holding the private key;
- 3) Upon the death of an Individual Subscriber; or
- 4) Upon the death or termination of employment of a Designated Certificate Holder.

The CA, in its discretion, may revoke a certificate when an Entity fails to comply with any agreement, any applicable law or where the CA reasonably believes it appropriate in the circumstances. The CA shall notify an Entity of any revocation of a certificate assigned to them.

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- 1) A Subscriber or Designated Certificate Holder;
- 2) An individual authorized to act on behalf of the Subscriber for whom the certificate was issued;
- 3) A Client Responsible Individual for a certificate issued to an individual, a role, device or application within a Client Organization;
- 4) CA personnel; or
- 5) An RA, at the request of a Subscriber or Client Responsible Individual.

4.4.3 Procedure for Revocation Request

The CA shall:

- 1) Authenticate all revocation requests;
- 2) Record and retain all information pertaining to such requests, including a statement as to the action taken by the CA;
- 3) Publish notice of the revocation of a certificate in its CRL.

4.4.4 Revocation Request Grace Period

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

- 1) Immediately, if the request is received during the CA's regular business hours;
- 2) Immediately upon the start of the next business day, if the request is received outside of regular business hours.

4.4.5 Circumstances for Suspension

The CA may effect the equivalent of a suspension by revocation where the reason code is "on hold". The temporary revocation of a certificate does not affect the obligations of a Subscriber with respect to the private key associated with the certificate.

The CA shall temporarily revoke a certificate upon the suspected compromise of the private key or the media holding the private key.

The CA, in its discretion, may temporarily revoke a certificate when an Entity fails to comply with any agreement, any applicable law or where the CA reasonably believes it appropriate in the circumstances.

4.4.6 Who can Request Suspension

The temporary revocation of a certificate may only be requested by:

- 1) A Subscriber or Designated Certificate Holder;
- 2) An individual authorized to act on behalf of the Subscriber for whom the certificate was issued;
- 3) A Client Responsible Individual or a Designated Certificate Holder within a Client Organization for a certificate issued to an individual, a role, device or application within that organization;
- 4) CA personnel; or
- 5) An RA upon the request of a Subscriber, Designated Certificate Holder or Client Responsible Individual.

4.4.7 Procedure for Suspension Request

The CA shall:

- 1) Authenticate all requests for the temporary revocation of certificates;
- 2) Record and retain all information pertaining to such requests, including a statement as to the action taken by the CA; and
- 3) Publish notice of any temporary revocation of a certificate in its CRL.

4.4.8 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.

4.4.9 CRL Issuance Frequency

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

4.4.10 CRL Checking Requirements

A Relying Party shall:

- 1) Check the status of all certificates in the certificate validation chain against the current CRLs prior to relying on such certificates; and
- 2) Verify the authenticity and integrity of CRLs.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

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:

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

5.1.2 Physical Access

With respect to the location of CA hardware and software, the CA shall ensure that:

- 1) Unescorted access to the CA server is limited to those personnel identified on an access list;
- 2) Personnel not on the access list are properly escorted and supervised; and
- 3) A site access log is maintained and inspected regularly.

The CA shall ensure all removable media and paper containing sensitive plaintext information is stored in containers either listed in, or of equivalent strength to those listed in, the GoC Security Equipment Guide.

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.

5.1.3 Power and Air Conditioning

The CA shall ensure that power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

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

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 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

- (1) Facilities used for off-site backup and archives have:
 - (a) The same level of security as the primary CA site; and
 - (b) Adequate protection from environmental threats such as temperature, humidity and magnetism.
- (2) The transmission and/or transport of material for backup and archiving from the CA to the off-site back-up facilities is done securely.

5.2 Procedural Controls

5.2.1 Trusted Roles

The CA shall enforce a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. Each user's system access will be limited to those actions that they are required to perform in fulfilling their responsibilities.

The CA shall provide for a minimum of three (3) distinct PKI personnel roles, distinguishing between day-to-day operations of the CA system; the management of those operations; and the management of substantial changes to system requirements including policies, procedures or personnel. These roles are to be performed by personnel designated as:

- a) PKI Master User;
- b) PKI Officer; and
- c) PKI Administrator,

and having, at a minimum, responsibilities as set out in Section 1.3.1. Any alternative division of responsibilities is permitted so long as it provides the same degree of resistance to "insider attack".

Only the PKI Master User and personnel responsible for the set up of the hardware and operating system software, or personnel escorted by them, are to have physical access to the software that controls the CA system.

CA personnel shall not audit their own activities.

5.2.2 Number of Persons Required per Task

The CA shall ensure that no single individual may gain access to Subscriber private keys stored by the CA. At a minimum, two individuals will perform any sensitive tasks, such tasks being defined in the CPS. The CA may permit Subscribers and Designated Certificate Holders to securely perform their own key recovery or certificate revocation operations.

Multi-user control is also required for CA key generation as outlined in Section 6.2.2. Subject to Section 5.2.1, one individual may perform all other duties associated with CA roles.

5.2.3 Identification and Authentication for Each Role

All CA personnel shall have their identity and authorization verified before they are:

- 1) Included in the access list for the CA site;
- 2) Included in the access list for physical access to the CA system;
- 3) Given a certificate for the performance of their CA role; and
- 4) Given an account on the PKI system if an account is required.

Any such certificate or account, with the exception of the CA signing certificate:

- 1) Shall be directly attributable to one individual;
- 2) Must not be shared with any other person; and
- 3) Shall not be used for any purposes other than those required to perform the duties assigned to the CA personnel holding such certificates or accounts.

The CA shall enforce these requirements through the use of CA and operating system software and procedural controls.

5.3 Personnel Controls

The CA will ensure that personnel performing duties with respect to the operation of the CA or a RA enter into employment contracts or otherwise acknowledge the terms and conditions of their employment. 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 2.5.1.

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

The CA shall ensure that all personnel associated with the operation of the CA are cleared and authorized to access Secret-level information.

5.3.2 Background Check Procedures

All background checks must be performed in accordance with the Government Security Policy.

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 at least once a year 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 these Certificate Policies, relevant provisions of the CPS, as well as any specific statutes, policies or contracts relevant to their positions to CA personnel, RAs and Client Responsible Individuals.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The CA shall ensure that it has the capacity to record or have recorded in audit log files all events relating to the security of the CA system, including but not limited to, routers, firewalls, directories and servers hosting CA and RA software. All security audit capabilities of the CA operating system and CA applications shall be enabled.

Such events include, but are not limited to:

- 1) System start-up and shutdown;
- 2) CA application start-up and shutdown;
- 3) Attempts to create, remove, set passwords or change the system privileges of the PKI Master User, PKI Officers and PKI Administrators;
- 4) Changes to CA details and/or keys;
- 5) Changes to certificate creation policies (e.g. validity period);
- 6) Login and logout attempts;
- 7) Unauthorized attempts at network access to the CA system;
- 8) Unauthorized attempts to access system files;
- 9) Generation of CA and subordinate entity keys;
- 10) Creation and revocation of certificates;
- 11) Attempts to initialize, remove, enable, and disable Subscribers, as well as attempts to update and recover their keys; and
- 12) Failed read-and-write operations on the certificate and CRL directory.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event.

The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- 1) Physical access logs;
- 2) System configuration changes and maintenance, as defined in the CPS;
- 3) CA personnel changes;
- 4) Discrepancy and compromise reports;
- 5) Information concerning the destruction of sensitive information;
- 6) Current and past versions of all Certificate Policies;
- 7) Current and past versions of Certification Practice Statements; and
- 8) Compliance Inspection Reports.

The CA shall indicate in the CPS what information is to be logged.

To facilitate decision making, all agreements and correspondence relating to CA services should be collected and consolidated, either electronically or manually, in a single location.

5.4.2 Frequency of Audit Log Processing

The CA shall ensure that all significant events are explained in an audit log summary and that CA personnel review audit logs at least once every week. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries. CA personnel shall conduct a more thorough investigation of any “alerts” or irregularities in the logs. 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 manual audit information from unauthorized viewing, modification, deletion or destruction.

5.4.5 Audit Log Back-up Procedures

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

5.4.6 Audit Collection System

The CA shall identify its audit collection system 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, organization, 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 following an examination of monitored events and shall take appropriate action to minimize identified system vulnerabilities as soon as reasonably possible.

5.5 Records Archival

Certificates, cross-certificates and CA (self-signed) certificates stored by the CA, as well as ARLs and CRLs generated by the CA, must be retained for at least two (2) years after their expiration.

Audit information, as detailed in Section 5.4, should be retained for a period to be defined in the Certification Practice Statement.

The following information must be retained for at least six (6) years:

- 1) Audit logs generated by the PKI CA software;
- 2) Subscriber agreements;
- 3) Records pertaining to identification and authentication information;
- 4) Physical access logs;
- 5) System configuration changes and maintenance, as defined in the CPS;
- 6) CA personnel changes;
- 7) Discrepancy and compromise reports;
- 8) Information concerning the destruction of sensitive information;
- 9) Current and past versions of all Certificate Policies;
- 10) Current and past versions of the Certification Practice Statement; and
- 11) Compliance Inspection Reports.

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.

Confidentiality private keys that are backed up by the CA shall be archived for a period of 10 years.

The CA shall archive any necessary keys and passwords for a period of time sufficient to support the responsibilities of the CA.

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.

The CA shall verify the integrity of back-ups once every six (6) months and the integrity of materials stored off-site once every year.

In addition to the foregoing, information retained or backed up by the CA may be subject to archival requirements, pursuant to the *National Archives of Canada Act*, other applicable legislation and GoC policy.

5.6 Key Changeover

The CA shall indicate in the CPS:

- 1) The period during which Subscriber and Designated Certificate Holder keys may be renewed prior to the certificate's expiry date, provided the certificate has not been revoked; and
- 2) The process by which the CA, an RA, Subscriber or Designated Certificate Holder may initiate key changeover.

Automated key changeover is permitted.

Subscribers and Designated Certificate Holders without valid keys must be re-authenticated in the same manner as initial registration.

The CA keys are automatically renewed at the frequency defined by section 6.3.2 of these Certificate Policies.

5.7 Compromise and Disaster Recovery

5.7.1 Computing Resources, Software and/or Data Corrupted

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.

5.7.2 CA Public Certificate Revocation

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

- 1) The FINTRAC PMA;
- 2) All of its RAs;
- 3) All Subscribers.

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

5.7.3 CA Key Compromise

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

- 1) Notify the FINTRAC PMA;
- 2) Revoke all certificates issued using that key; and
- 3) Provide appropriate notice to all relevant parties.

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

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

5.7.4 Business Continuity Capabilities After a Disaster

The CA shall prepare and maintain a business continuity plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster.

The business continuity plan should address:

- 1) The definition of roles and responsibilities of those responsible for executing various components of the plan;
- 2) The conditions for activating the plan, describing the process to be followed before the plan is activated;
- 3) Emergency procedures describing the action to be taken following an incident that jeopardizes business operations and/or human life.
- 4) Fallback procedures, describing the actions to be taken to move essential business activities or support services to alternative locations, and to bring business processes back into operation in required time-frames;
- 5) Resumption procedures, describing the actions to be taken to return to normal business operations;
- 6) A maintenance schedule, specifying how and when the plan will be tested, as well as the process for maintaining the plan; and
- 7) Awareness and education activities, designed to create understanding of the business continuity processes and ensure that the processes continue to be effective.

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 Termination/Change in Operations

In the event the CA ceases operation or makes a major change in operations, the CA shall notify the FINTRAC PMA as to all Entities for which it has issued certificates, such notice shall be given prior to or immediately upon the termination of operations or major change in operations.

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

- 1) Certificates;
- 2) Confidentiality private keys (if applicable);
- 3) CA self-signed certificates;
- 4) CRLs;
- 5) Audit information detailed in Section 5.4;

in accordance with archival requirements specified in these Certificate Policies.

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

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 FINTRAC PMA approved algorithm.

RA Key Generation

The CA shall ensure that RA key generation shall be:

- a) Carried out within a device which satisfies the requirements identified in Section 6.2.1 or higher; and
- b) Performed using a FINTRAC PMA approved algorithm.

Subscriber/Designated Certificate Holder Key Generation

DIGITAL SIGNATURE	CONFIDENTIALITY
Each digital signature key pair must be generated using an algorithm approved by the FINTRAC PMA.	Each confidentiality key pair must be generated using an algorithm approved by the FINTRAC PMA.

Where a key pair is generated on behalf of a prospective certificate holder, the entity or process that generated the keys must destroy their copy of the key pair in a secure manner following the placement of the keys in the custody of the prospective certificate holder.

Key pairs for End-Entities, other than the CA, may be generated in a software or hardware cryptographic module.

6.1.2 Private Key Delivery to Subscriber/Designated Certificate Holder

DIGITAL SIGNATURE	CONFIDENTIALITY
If the prospective certificate holder does not generate the private signing key, the CA shall place the key in storage in a manner that ensures that only the prospective certificate holder has access to it.	If the prospective certificate holder does not generate the private decryption key, the CA shall place the key in storage.

6.1.3 Public Key Delivery to Certificate Issuer

DIGITAL SIGNATURE	CONFIDENTIALITY
If the CA does not generate the public verification key, the CA shall arrange for its delivery to the CA in an on-line transaction in a secure manner documented in the CPS.	If the CA does not generate the public encryption key, the CA shall arrange for its delivery to the CA in an on-line transaction in a secure manner documented in the CPS.

6.1.4 CA Public Key Delivery to Subscribers

The CA public verification key will be delivered to Subscribers and Designated Certificate Holders in an on-line transaction in a secure manner documented in the CPS.

6.1.5 Key Sizes

The CA shall use a minimum of a 1024 bit RSA (2048 bit RSA recommended) for its own CA signing key pair. Where possible, End Entities shall use 2048 bit RSA for their key pairs. Where this is not practical, End Entities shall use 1024 bit RSA for their key pairs.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per x509v3 field)

DIGITAL SIGNATURE	CONFIDENTIALITY
<p>Keys may be used for authentication and data integrity and in support of non-repudiation. CA signing keys are the only keys permitted to be used for signing certificates and CRLs.</p> <p>The certificate KeyUsage field must be used in accordance with the GoC X.509 Certificate and CRL Fields and Extensions Profile.</p>	<p>Keys may be used for exchange and establishment of keys used for session and data confidentiality.</p> <p>The certificate KeyUsage field must be used in accordance with the GoC X.509 Certificate and CRL Fields and Extensions Profile.</p>

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Any cryptographic module used by the CA, CA personnel, RAs, Subscribers and Designated Certificate Holders must satisfy the following requirements:

- 1) 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 140-1 level 3 or otherwise deemed to provide an equivalent level of functionality and assurance.
- 2) All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise deemed to provide an equivalent level of functionality and assurance.

- 3) RAs Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 1 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 140-1 Level 1 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. All other RA cryptographic operations must be performed in cryptographic modules rated FIPS 140-1 Level 1 or otherwise deemed to provide an equivalent level of functionality and assurance.
- 4) End Entities must use cryptographic modules validated to at least FIPS 140-1 Level 1 or otherwise deemed to provide an equivalent level of functionality and assurance.
- 5) All cryptomodules must automatically lock after a specific period of inactivity.

6.2.2 Private Key Multi-person Control

DIGITAL SIGNATURE	CONFIDENTIALITY
There must be multiple person control for CA key generation operations. Two individuals, one of whom performs the duties associated with the role of PKI Master User, must participate or be present.	There must be multiple person control for private key recovery. Two individuals, one of whom performs the duties associated with the roles of PKI Officer or PKI Administrator, must participate or be present.

6.2.3 Private Key Escrow

DIGITAL SIGNATURE	CONFIDENTIALITY
The CA shall not escrow Digital Signature private keys.	No stipulation.

6.2.4 Private Key Back-up

DIGITAL SIGNATURE	CONFIDENTIALITY
<p>An Entity may back-up its own private digital signature signing key. If so, the key must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.</p> <p>The CA shall not back-up private signing keys of the Subscribers or Designated Certificate Holders.</p>	<p>An Entity may also make a back up of its private decryption key.</p> <p>If confidentiality keys are backed up by the CA, the CA shall store backed-up keys in encrypted form and securely store them.</p>

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

6.2.5 Private Key Archival

Refer to Section 5.5.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

DIGITAL SIGNATURE	CONFIDENTIALITY
If a private signing key is not generated in the Entity's cryptographic module, it must be entered into the module in a secure manner.	If a private decryption key is not generated in the Entity's cryptographic module, it must be entered into the module in a secure manner.

6.2.7 Private Key Storage on Cryptographic Module

Private keys shall be stored in a PSE.

6.2.8 Method of Activating Private Key

An Entity must be authenticated to the PSE before the activation of the private key. The CA shall ensure that a password policy rules are in place to require the use of strong passwords to access a PSE. The FINTRAC PMA 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.

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. Since keys are held in an encrypted PSE, the deletion of the PSE or physical destruction of any token (if applicable) constitutes a secure method of destroying the private key.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

DIGITAL SIGNATURE	CONFIDENTIALITY
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 Pair Usage Periods

Key/Certificate	Key Length in Bits	Maximum Validity Period
Certification Authority Public Verification Key and Certificate	1024/2048	8/20 years
Certification Authority Private Signing Key	1024/2048	3/8 years

Key/Certificate	Key Length in Bits	Maximum Validity Period
End Entity Public Verification Key and Certificate	2048	12 years
End Entity Private Signing Key	2048	3.2 years
End Entity Public Encryption Key and Certificate	2048	12 years
End Entity Private Decryption Key	2048	No expiry
End Entity Public Verification Key and Certificate	1024	6 years
End Entity Private Signing Key	1024	3.2 years
End Entity Public Encryption Key and Certificate	1024	6 years
End Entity Private Decryption Key	1024	No Expiry

6.3.3 CA Key Storage, Backup and Recovery

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

- 1) 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;
- 2) 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;
- 3) When outside the signature-creation device, the CA private signing key shall be encrypted;
- 4) 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;
- 5) 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.

6.3.4 Key Recovery by Subscriber or Designated Certificate Holder

The CA may allow a Subscriber or Designated Certificate Holder to recover their keys.

6.4 Activation Data

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. Upon receipt of the digital signature key pair and associated initialization data, a Subscriber or Designated Certificate Holder must use the initialization data in a timely manner.

6.4.2 Activation Data Protection

Data used for Entity initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

The Personal Security Environment of Entities must be protected from unauthorized use by cryptographic mechanisms.

The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, the CA shall ensure that PKI system and/or applications enforce a strong password policy. The level of protection must be adequate to deter a motivated attacker with substantial resources.

If a reusable password scheme is used, the mechanism shall include a facility to temporarily lock the account after a predetermined number of login attempts.

An Entity must have the capability to change its password at any time.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA server must include the following security functionality:

- 1) Access control to CA services and PKI roles;
- 2) Enforced separation of duties for PKI roles;
- 3) Identification and authentication of PKI roles and associated identities;
- 4) Object reuse controls or separation for CA random access memory;
- 5) Where required, use of cryptography for session communication and database security;
- 6) Archival of CA and End-Entity history and audit data;
- 7) Audit of security related events;
- 8) Automatic and regular validation of CA database integrity;
- 9) Trusted path mechanisms for the identification and authentication of PKI roles and associated identities;
- 10) Recovery mechanisms for keys and the CA system; and
- 11) 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.

6.5.2 Computer Security Rating

The Communications Security Establishment (CSE) or any other accredited third party laboratory must evaluate the security critical elements of the CA.

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 be supported by third party verification of process compliance 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 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:

- 1) Originated from the software developer;
- 2) Has not been modified prior to installation; and
- 3) Is 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.

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

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 AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version Number

The CA shall issue X.509 version 3 certificates or a later version of X.509 certificates if such use is approved by the FINTRAC PMA.

The PKI End-Entity software must support all the base (non-extension) X.509 fields:

Field Name	Description
Signature	CA signature to authenticate certificate
Issuer	Name of CA
Validity	Activation and expiry date for certificate
Subject	Subscriber's Distinguished Name
Subject Public Key Information	Algorithm ID key
Version	Version of X.509 certificate
Serial Number	Unique serial number for certificate

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 these Certificate Policies shall conform to the applicable parts of the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile.

The CAs shall post the GoC PKI X.509 Certificate and CRL Fields and Extension Profile on its Web site and advise Subscribers and Designated Certificate Holders of its location. Where private extensions are used, they shall be identified in its CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

The CA and End Entities shall only use algorithms approved by the FINTRAC PMA. The CA shall use and End Entities must support the following symmetric algorithms:

Encryption	
Algorithm	Comments
<i>Triple DES</i>	<p>The 3 independent key option provides the best security and is therefore the preferred option. The 2-key option is also acceptable, where the key used in the final encryption is the same as in the first encryption.</p> <p>The single key option is not acceptable, as it reduces the security to that of a single-pass DES.</p> <p>The cryptoperiod of any one key should not exceed seven days.</p>
<i>CAST 5/80 or CAST 5/128</i>	<p>Acceptable modes of operation are the same as those originally specified for DES.</p> <p>The cryptoperiod of any one key should not exceed twenty-four hours.</p>

The list of symmetric algorithms to be used by all PKI Entities may change without triggering the issuance of a new Certificate Policy or a change in the CP's OID.

In the event of any change in approved algorithms, the CA shall ensure that Subscribers and Designated Certificate Holders are made aware of changes in the list of algorithms approved for use with FINTRAC. The CA shall indicate in its CPS the manner in which it will provide such notice of change.

7.1.4 Name Forms

Every DN must be in the form of an X.501 printableString.

7.1.5 Name Constraints

When used, the name constraints extension shall be populated and processed as described in the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile.

7.1.6 Certificate Policy Object Identifier

The CA shall ensure that the applicable Policy OID is contained within the certificates it issues.

7.1.7 Usage of Policy Constraints Extension

When used, the policyConstraint extension shall be populated and processed as described in the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile.

7.1.8 Policy Qualifiers Syntax and Semantics

When used, the policyQualifiers extension shall be populated and processed as described in the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile.

7.1.9 Processing Semantics for Critical Certificate Extensions

Critical extensions, when marked, shall be interpreted as defined in the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile.

7.2 CRL Profile

7.2.1 Version Number

The CA shall issue X.509 version two (2) CRLs and ARLs or a later version of X.509 CRLs and ARLs if such use is approved by the FINTRAC PMA. 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 Entity PKI software must correctly process all CRL extensions identified in the GoC PKI X.509 Certificate and CRL Fields and Extensions Profile. The CA shall state in its CPS the use of any extensions supported by the CA, its RAs and End Entities.

8. COMPLIANCE INSPECTION AND OTHER ASSESSMENTS

A compliance inspection determines whether the CA's performance meets the requirements established by these Certificate Policies and associated CPS.

A compliance inspection of the CA will be conducted on such terms and conditions as may be established by the FINTRAC PMA. Compliance inspection reports shall not be made public unless required by agreement or pursuant to judicial authorization or an express statutory requirement.

8.1 Frequency or Circumstances of Assessment

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

A qualified inspector external to the CA shall conduct one (1) of every five (5) inspections of the CA. The FINTRAC PMA may order a compliance inspection by an agency external to the CA at any time.

The CA will certify annually to the FINTRAC PMA that it has at all times during the period in question complied with the requirements of these Certificate Policies and will provide reasons where it has not complied with these Certificate Policies and state any periods of non-compliance.

8.2 Identity and Qualifications of Assessor

The inspector must demonstrate competence in the field of compliance inspections, and must be familiar with the requirements that the FINTRAC PMA imposes on the issuance and management of certificates issued under these Certificate Policies.

8.3 Assessor's Relationship to Assessed Entity

An inspector must be independent of the management or operation of the CA.

An inspector who is external to FINTRAC must be independent of the CA and, if applicable, must comply with the provisions of the Conflict of Interest and Post-Employment Code for Public Office Holders or the Conflict of Interest and Post-Employment Code for the Public Service.

8.4 Topics covered by Assessment

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

- 1) The CPS outlines, in sufficient detail, the technical, procedural and personnel practices of the CA required under these Certificate Policies;
- 2) The CA implements and complies with those technical, procedural and personnel practices; and
- 3) The Repository Manager, RAs and Client Responsible Individuals implement and comply with the technical, procedural and personnel practices set out by the CA.

The FINTRAC PMA may increase the scope of a compliance inspection on such terms as it deems appropriate.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

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