Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

CERTIFICATE POLICY

DIGITAL SIGNATURE

RUDIMENTARY ASSURANCE LEVEL

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

id-gocpki-certpcy-digitalSignature-rudimentaryAssurance ::=
id-gocpki-certpcy-sign-1

VERSION 3.02
APRIL 1999

Canada

TABLE OF CONTENTS

PART 1 – BACKGROUND

PART 2 – POLICY SPECIFICATION

PART 1 – BACKGROUND

1. INTRODUCTION

This document defines the Digital Signature certificate policy – rudimentary assurance level – for use in the Government of Canada Public Key Infrastructure (GOC PKI). The Policy Specification portion of the document (Part 2) follows and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

This document explains several technical concepts associated with PKI technology. For those unfamiliar with this technology a series of definitions is provided in introduction of the policy specification.

The security mechanisms provided by the GOC PKI alone are not intended to be used for the protection of classified information.

2. CONCEPTS

2.1 Certificate Policy

When a Certification Authority (CA) issues a certificate, it provides a statement to a certificate user that a particular public key is bound to a particular Entity. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes. The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Because of the importance of a Certificate Policy (CP) in establishing trust in a public key certificate, it is fundamental that the CP be understood and consulted not only by Subscribers but any Relying Party.

GOC PKI certificates contain a registered certificate policy object identifier (OID), which may be used to decide whether or not a certificate is trusted for a particular purpose. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID also publishes the CP, for examination by certificate users and other parties. Each GOC PKI certificate must refer to a CP but may also refer to other non-conflicting CPs. For example, a GOC PKI certificate may support multiple assurance levels for either digital signature or confidentiality but not support both digital signature and confidentiality.

Certificate policies constitute a basis for accreditation of CAs. Each CA is accredited to support one or more CPs, which it proposes to implement.

Certificate policies are also used to establish a trust relationship between CAs (cross-certification). When CAs issue cross-certificates, one CA assesses and recognizes one or more certificate policies of the other CA. When a trust relationship is established directly between two CAs or indirectly through intermediate CAs, the X.509 certification path processing logic is employed to identify a common certificate policy.

2.2 Certification Practice Statement

The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA.

A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, a number of CAs, with non-identical CPSs, may support the same certificate policy.

2.3 Relationship between a Certificate Policy and a Certification Practice Statement

A CP states what assurance can be placed in a certificate. A CPS states how a CA establishes that assurance. A certificate policy may apply more broadly than to just a single organization; a CPS applies only to a single CA.

Certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria industry-wide (or possibly more global). A detailed CPS alone does not form a suitable basis for interoperability between CAs operated by different organizations.

3. ILLUSTRATIVE GOC PKI ROLES

The operation of a Certification Authority requires the assignment of certain roles with corresponding responsibilities. The CPS should state clearly who within an organization has been assigned specific roles and state their respective responsibilities. Possible roles and responsibilities are illustrated in the table below.

ROLE	LOCATION	RESPONSIBILITIES
Policy Management Authority		• Sets, implements and administers policy for the PKI
Operational Authority	Certificate Authority (CA)	• Overall responsibility for the operation of the CA
PKI Master User	Certificate Authority (CA)	• Initial configuration and on-going maintenance of the CA application software and hardware • Starting and stopping of CA services • Initial creation of accounts for PKI Officers

ROLE	LOCATION	RESPONSIBILITIES
PKI Officer	Certificate Authority (CA)	• Managing PKI Administrators, Local Registration Authority Administrators (account creation, modification and removal) • Audit of operational logs • Verification of certificate policy and CPS compliance • Subscriber key recovery
PKI Administrator	Within the Certificate Authority (CA) protected LAN	• PKI Subscriber administration local to the CA
Local Registration Authority (LRA)	Local Registration Authority (outside the protected LAN)	• PKI Subscriber administration remote from the CA
Local Registration Authority (LRA) Administrator	Local Registration Authority (outside the protected LAN)	• PKI Subscriber administration remote from the CA through the use of an LRA application that assigns key material in an on-line interaction with the CA
Sponsor	Department	• Notifying/verifying CA/LRA of a Subscriber's right to a certificate and any relevant credentials of the Subscriber • Notifying the CA/LRA when a Subscriber's certificate is to be updated or revoked
Directory Administrator	Directory	• Managing the directory used by the CA, in particular for creating and updating directory entries for each Subscriber
System Administrator	Certificate Authority (CA)/Local Registration Authority (LRA)	• Set-up of the hardware and operating system software

PART 2 – POLICY SPECIFICATION

1. INTRODUCTION

1.1 Overview

The certificate policy defined in this document is intended for use by departments and agencies of the Government of Canada. Users of this document are to consult the issuing Certification Authority to obtain further details of the implementation of this Certificate Policy. There are eight policies: four with respect to Digital Signature certificates and four with respect to Confidentiality certificates. The applicability of these certificates will depend on the application used.

The four PKISignCertPcy policies are for the management and use of certificates containing public keys used for verification, authentication, integrity and key agreement mechanisms. For instance, the certificates issued under these policies could be used for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of citizens or other legal entities, or protecting the integrity of software and documents.

The four PKIConfidentialityCertPcy policies are for the management and use of certificates containing public keys used for encryption key establishment, including key transfer. The certificates issued under these policies are suitable for providing confidentiality for applications such as electronic mail or Web communications, including the protection of GSP designated information. They are not to be used for protection of classified information.

The term “assurance” is not intended to convey any representation or warranty as to 100% availability of CA services offered under the GOC PKI. System maintenance, system repair or factors outside the control of the CA may affect such availability. The Government of Canada does not represent or warrant 100% availability offered under the GOC PKI.

Issuance of a public key certificate under any of these policies does not imply that the Subscriber has any authority to conduct business transactions on behalf of the organization operating the CA.

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

The Government of Canada reserves the right not to enter into a cross-certification agreement with an external Certification Authority.

1.1.1 Policy overview

The Policy Object Identifier Designation for this Policy is _____.

A CA is not required to maintain a public repository for this type of certificate but is obliged to make a certificate available to a Subscriber.

The use of rudimentary assurance level confidentiality keys is not appropriate for the confidentiality of designated information.

The Crown in right of Canada disclaims all liability for any use of this type of certificate. Any disputes concerning key or certificate management under this policy are to be resolved by the Department issuing the policy.

Certificates may be issued under this policy without any authentication of a Subscriber's identity. Identification may be in any manner indicated by the CA.

A CA is not obliged to revoke certificates under this type of policy.

A CA is not obliged to maintain a Certificate Revocation List for this type of certificate.

A CA is not obliged to maintain records or information logs for this type of certificate.

A CA may permit all critical CA functions to be performed by one individual.

Digital signature keys must not be backed-up or otherwise stored. Keys may have a validity period of no more than one (1) year if CRLs are NOT used and six (6) years if CRLs are used.

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law.

CA activities are subject to inspection.

1.1.2 General definitions

Accreditation Authority – A PKI management Entity with the authority to permit a subordinate PKI Entity to operate within a particular domain. The PMA is the accreditation authority for all connections to the GOC PKI. A particular unit or section within a Department may be assigned the role of accreditation authority for the level 1 CA within that Department.

Activation Data – Private data, other than keys, that are required to access cryptographic modules.

Authority Revocation List (ARL) – A list of revoked CA certificates. An ARL is a CRL for CA cross-certificates.

Canadian Central Facility – The Government of Canada PKI central Certification Authority. Under direction from the PMA the CCF signs and manages the cross-certificates of GOC departmental top level CAs. The CCF also signs and manages cross-certificates with non-GOC CAs. The CCF does not manage any Subscriber certificates.

Certificate – The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate Revocation List (CRL) – A list maintained by a Certification Authority of the certificates that it has issued that are revoked before their natural expiry time

Certification Authority – An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs. Each CA within the GOC PKI may issue certificates under a choice of policies based on the assurance level the CA has been accredited to and the requirements and role of the Subscriber.

Certification Authority Software – The cryptographic software required to manage the keys of end entities.

Cross-Certificate – A certificate used to establish a trust relationship between two Certification Authorities.

Data Integrity – Assurance that the data are unchanged from creation to reception.

Department – A department is any body as identified in Schedule I, Parts I and II of the *Public Service Staff Relations Act*; the Canadian Forces; and the Royal Canadian Mounted Police.

Digital Signature – The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

(a) whether the transformation was created using the key that corresponds to the signer's key; and

(b) whether the message has been altered since the transformation was made.

Employee – An employee is any person employed by a "department" as defined above.

End-Entity – An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End-Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity – Any autonomous element within the Public Key Infrastructure. This may be a CA, an LRA or an End-Entity.

Issuing CA – In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

Level One CA – The highest level CA within a department. Level One CAs are cross-certified with the CCF and may also be cross-certified with subordinate departmental (Level Two) CAs.

Local Registration Authority (LRA) – A person or organization that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign or issue the certificates. A LRA is delegated certain tasks on behalf of a CA.

MD5 – One of the message digest algorithms developed by RSA Data Security Inc.

Object Identifier – (OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the GOC PKI they are used to uniquely identify each of the eight policies and cryptographic algorithms supported.

Operational Authority – Departmental personnel who are responsible for the overall operation of a GOC PKI CA.

Organization – A department, agency, corporation, partnership, trust, joint venture or other association or governmental body.

Policy Management Authority – A GOC body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the GOC PKI.

Public Key Infrastructure – A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and keys.

Relying Party – A person who uses a certificate signed by a GOC PKI CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a Subscriber of a GOC PKI CA or a PKI that is cross-certified with the GOC PKI.

Repository – A location where CRLs, ARLs and certificates are stored for access by End-Entities.

Sponsor – A Sponsor in the GOC PKI is the department or public servant that has nominated that a specific individual or organization be issued a certificate. (e.g., for an employee this may be the employee's manager). In the case of a certificate for a citizen or a commercial enterprise the Sponsor could be the manager of the GOC business unit that has a requirement to communicate with that Entity. The Sponsor might suggest an appropriate DN for the certificate and will be responsible for either supplying or confirming the certificate attribute details to the LRA. The Sponsor is also responsible for informing the CA or LRA if the department's relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subscriber – An individual or organization whose public key is certified in a public key certificate. In the GOC PKI this could be a public servant, a citizen, or a government client or supplier. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature verification key; the other containing their Confidentiality encryption key.

1.1.3 Government security policy definitions

Classified – Information when if compromised could reasonably be expected to cause injury to the national interest. Information of this type is generally marked as CONFIDENTIAL, SECRET, or TOP SECRET according to the gravity of injury.

Enhanced Reliability Check (ERC) – An assessment to determine an individual's trustworthiness; condition for enhanced reliability status.

Extremely sensitive – Applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life. Information of this type may be marked ***PROTECTED C***.

High-security Zone – An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter built to the specifications recommended in the TRA. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

Low- sensitive – Applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure. Information of this type may be marked ***PROTECTED A***.

Operations Zone – An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

Particularly sensitive – Applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example loss of reputation or competitive advantage. Information of this type may be marked ***PROTECTED B***.

Public-access Zone – Generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorized activity.

Reception Zone – The entry to a facility where the initial contact between the public and the department occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognisable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.

Security Zone – An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

1.1.4 Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CCF	Canadian Central Facility
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DN	Distinguished Name
ERC	Enhanced Reliability Check
FIPS PUB	(US) Federal Information Processing Standard Publication
GOC	Government of Canada
GSP	Government Security Policy, Government of Canada
ITU	International Telecommunications Union
IETF	Internet Engineering Task Force
LRA	Local Registration Authority
NIST	National Institute of Standards and Technology
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm
TRA	Threat and Risk Assessment
URL	Uniform Resource Locator

1.2 Identification alphanumeric OID

id-gocpki-certpcy-digitalSignature-rudimentaryAssurance ::= {id-gocpki-certpcy-sign-1}

1.3 Community and applicability

These certificate policies have been designed to satisfy general public key certificate requirements of the Government of Canada.

GOC PKI CAs are not obligated to issue, recognize or support all eight policies. They are also not limited to only these policies, in that any GOC CA may issue, recognize or support additional certificate policies.

1.3.1 Certification Authorities (CAs)

A CA operating under this policy is responsible for the creation and signing of certificates binding Subscribers with their signature verification keys.

While a department may use a contractor to provide CA services, it must remain responsible and accountable for the operation of its CA.

GOC PKI Level One CAs will cross-certify only with the CCF. A cross-certification must be in accordance with the selected certificate policy and any additional requirements determined by the PMA. All cross-certification between GOC PKI CAs and non-GOC CAs will be done through the CCF pursuant to instructions from the PMA. Any agreements made with other CAs must be documented and applicable disclaimers made available to Subscribers.

A CA may issue cross-certificates to other GOC CAs where expressly authorized by the GOC PMA.

1.3.2 Local Registration Authorities (LRAs)

LRAs are not required for issuance of Rudimentary Assurance certificates as registration can be performed on-line directly between the CA and the End-Entity.

1.3.3 Repositories

A public repository is not required for this type of certificate.

1.3.4 Subscribers

Individuals or organizations may be Subscribers. Subscribers may be issued certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability is attributable to an individual or an organization.

GOC PKI certificates will only be issued after request or authorisation for issuance from one or more Sponsors. They may be issued to employees, citizens, organizations or others with whom the Sponsor has relationship.

Eligibility for a certificate is at the sole discretion of the CA.

A CA may administer any number of Subscribers.

1.3.5 Relying parties

No stipulation.

1.3.6 Policy applicability

This policy is intended for certificate use such as the authentication of relationships (but not authentication of identities) between a Subscriber and a department.

1.3.6.1 Approved and prohibited applications

A CA must advise Subscribers which applications are intended to be used with the PKI system. These applications must, as a minimum, meet the following requirements:

- correctly establish, transfer and use the public and private keys;
- are capable of performing the appropriate certificate validity and verification checking; and
- report appropriate information and warnings to the Subscriber.

1.4 Contact details

The Government of Canada PKI Policy Management Authority, Treasury Board Secretariat, Ottawa, Ontario, Canada administers this certificate policy.

The contact person is:

Chairman, Government of Canada PKI Policy Management Authority
Treasury Board Secretariat, 275 Slater Street, 6th floor, Ottawa, Ontario K1A 0R5
Fax: (613) 946-9893, E-mail: pki-icp@tbs-sct.gc.ca.

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The CA will operate in accordance with its CPS, this CP, and the laws of Canada when issuing and managing the keys provided to LRAs and Subscribers under this CP. The CA will ensure that all LRAs operating on its behalf will comply with the relevant provisions of this CP concerning the operation of LRAs. The CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End-Entity hardware and software used in connection with the PKI.

A CA must provide notice of limitations of liability. Such notice must, at a minimum, be provided within the certificate either through a private certificate extension or the use of the `userNotice` field within the certificate as defined by PKIX. Because of space limitations within a certificate, such notice must be limited to the following language: "Limited Liability. See CP-Responsabilité limitée. Voir PC".

A CA must:

- issue a CPS;
- have in place mechanisms and procedures to ensure that its LRAs and Subscribers are aware of, and agree to abide with, the stipulations in this policy that apply to them;
- establish that any CA with whom it cross-certifies complies with all CPs that are mutually recognized; and
- through compliance inspection, verify to cross-certifying CAs that it complies with this CP.

CA personnel associated with PKI roles (e.g. PKI Administrators, PKI Master Users, and PKI Officers) must be individually accountable for actions they perform. "Individually accountable" means that there must be evidence that attributes an action to the person performing the action.

2.1.1.1 Notification of certificate issuance and revocation

An Issuing CA is required to make a certificate available to the Subscriber.

A CA is not required to make CRLs available to a Subscriber or Relying Party unless otherwise stated in the Subscriber agreement.

2.1.1.2 Accuracy of representations

When an Issuing CA publishes a certificate it certifies that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP. Publication of the certificate in a repository, to which the subscriber has access, constitutes notice of such verification.

A CA will provide to each Subscriber notice of the Subscriber's rights and obligations under this Certificate Policy. Such notice may be in the form of an agreement for non-GOC employees or an acceptable use policy for GOC employees. Such notice will include a description of the allowed uses of certificates issued under this CP; the Subscriber's obligations concerning key protection; and procedures for communication between the Subscriber and the CA or LRA, including communication of changes in

service delivery or changes to this policy. Subscribers should also be notified as to procedures for dealing with suspected key compromise, certificate or key renewal, service cancellation, and dispute resolution.

A CA will ensure that any notice of the Subscriber's rights and obligations under this Certificate Policy includes a description of a Relying Party's obligations with respect to use, verification and validation of certificates.

2.1.1.3 Time between certificate request and issuance

No stipulation.

2.1.1.4 Certificate revocation and renewal

No stipulation.

2.1.1.5 Protection of private keys

All Entities must ensure that their private keys and activation data are protected in accordance with 4 and 6.

2.1.1.6 Restrictions on issuing CA's private key use

A CA must ensure that its certificate signing private key is used only to sign certificates and CRLs. A CA may issue certificates to Subscribers, CA and LRA personnel, devices and applications. CA may issues cross-certificates in accordance with 1.3.1.

A CA must ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes. If required, its personnel would be issued sets of Subscriber keys and certificates to be used for purposes other than CA use.

2.1.2 LRA obligations (LRA duties)

Not applicable.

2.1.2.1 Notification of certificate issuance and revocation

Not applicable.

2.1.2.2 Accuracy of representations

Not applicable.

2.1.2.3 Protection of LRA private keys

Not applicable.

2.1.2.4 Restrictions on LRA private key use

Not applicable.

2.1.3 Subscriber obligations

An Issuing CA must ensure that a Subscriber enters into an agreement or abides by an acceptable use policy which outlines the terms and conditions of use, including permitted applications and purposes.

2.1.3.1 Representations

Any information required to be submitted to a CA or LRA in connection with a certificate must be complete and accurate.

2.1.3.2 Protection of subscriber private key and key token

Subscribers are required to protect their private keys and key tokens (if applicable) in accordance with 6, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

2.1.3.3 Restrictions on End-Entity private key use

The Subscriber will use the keys and certificates only for the purposes identified in the CP.

2.1.3.4 Notification upon private key compromise

No stipulation.

2.1.4 Relying party obligations

The rights and obligations of a Relying Party who is a member of the GOC PKI are covered in this policy. The rights and obligations of a Relying Party belonging to another PKI must be addressed in the cross-certification agreement between the two PKIs.

2.1.4.1 Use of certificates for appropriate purpose

Prior to using a Subscriber's certificate, a Relying Party must ensure that it is appropriate for the intended use.

2.1.4.2 Verification responsibilities

A Relying Party must use certificates only in accordance with the certification path validation procedure specified in X.509 and PKIX.

2.1.4.3 Revocation check responsibility

No stipulation.

2.1.5 Repository obligations

No stipulation.

2.2 Liability

2.2.1 Requirements

An Issuing CA will ensure that its certification and repository services, issuance and revocation of certificates, and issuance of CRLs is in accordance this CP. It will also take reasonable efforts to ensure that all LRAs and Subscribers will follow the requirements of this policy when dealing with any certificates containing this policy's OID or the associated keys.

2.2.2 Disclaimers of warranties and obligations

The Crown, in right of Canada assumes no liability whatsoever in relation to the use of GOC PKI certificates or associated public/private key pairs for any use other than in accordance with this CP and any other agreements, and Subscribers will indemnify the Crown and save the Crown harmless from any such liability.

The Crown in right of Canada, its employees, servants or agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or in any other document.

No joint venture, partnership, trust, agency or fiduciary relationship is established or deemed to be established between the Crown and its citizens, trading partners or others using the GOC PKI.

2.2.3 Limitations of liability

The Crown, in right of Canada, disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, a GOC PKI rudimentary certificate or its associated public/private key pair.

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

2.2.4 Other terms and conditions

The disclaimers and limitations of liability in 2.2.2 and 2.2.3 are subject to any signed contract or cross-certification agreement that may be entered into by the Crown that provides otherwise. Any such disclaimers or limitations of liability must be consistent with this Certificate Policy.

2.3 Financial responsibility

A CA which contracts for the provision of its CA services must require that any CA it uses provides satisfactory evidence of financial responsibility and waiver of any legislative immunity, if applicable.

2.4 Interpretation and Enforcement

2.4.1 Governing law

A CA must ensure that any agreements by that CA will be governed by the laws of Canada and applicable provincial law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

2.4.2 Severability, survival, merger, notice

A CA must ensure that any agreements by that CA will contain appropriate provisions governing severability, survival, merger or notice.

2.4.3 Dispute resolution procedures

Disputes related to key and certificate management are resolved by the appropriate departmental authority in conjunction with the Issuing CA.

2.5 Fees

The charging of fees is subject to appropriate legislative authority and policy. Notice of any fee charged to a Subscriber or Relying Party must be brought to the attention of that Entity.

2.6 Publication and repository

An issuing CA must:

- include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA;
- ensure the publication of its CP, digitally signed by an authorized representative of the CA, on a web site maintained by, or on behalf, of the CA, the location of which must be indicated in compliance with 8;
- ensure, directly or through agreement with a repository, that operating system and repository access controls will be configured so that only authorized CA personnel can write or modify the online version of the CP; and
- provide a full text version of the CPS when necessary for the purposes of any audit, inspection, and accreditation or cross-certification.

Access controls may be instituted at the discretion of the CA with respect to certificates or on-line certificate status (if the latter is provided as a service by the CA). Certificates must be published promptly upon issuance. A CA must ensure, directly or with agreement with a repository, unrestricted access to CRLs. CRL publication must be in accordance with 4.

2.7 Compliance inspection

A compliance inspection determines whether a CA's performance meets the standards established in its CPS and satisfies the requirements of the CPs it supports.

2.7.1 Frequency of compliance inspection

A CA issuing certificates pursuant to the CP must establish to the satisfaction of any CA with whom it cross-certifies that it fully complies with the requirements of this policy:

- prior to initial cross-certification with a GOC PKI CA; and
- as a minimum every three years thereafter.

2.7.2 Identity/qualifications of CA inspector

Any person or entity, external to the GOC, seeking to perform a compliance inspection must possess significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

2.7.3 Inspector's relationship to audited CA

Where an inspector is within the GOC, the inspector must be independent of the CA.

Where an inspector is external to the GOC, the inspector must be independent of the CA and 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. No person may be appointed an inspector to perform an inspector who is, whose partner is, or a member of whose firm is:

(i) a member of the relevant Minister's family;

(ii) a member of the family of another Minister or of colleagues in the House of Commons or Senate; or

(iii) employed in, or a member of the immediate family of, a person referred to above where such family members are employed in a senior position of authority in a non-government organization.

No member of the House of Commons or the Senate shall be admitted to share any part of a contract between the inspector and the Government of Canada, nor any resulting benefit.

2.7.4 Topics covered by inspection

The compliance inspection must follow the inspection guidelines instituted by PMA. This will include whether:

- the CPS outlines, in sufficient detail, the technical, procedural and personnel policies and practices of the CA which meet the requirements of all the certificate policies supported by the CA;
- the CA implements and complies with those technical, procedural and personnel practices and policies; and
- an LRA, if used, implements and complies with those technical, procedural and personnel practices and policies set out by the CA.

2.7.5 Actions taken as a result of inspection

The inspection results must be submitted to the accreditation authority and PMA. If irregularities are found, the CA must submit a report to the accreditation authority and PMA as to any action the CA will take in response to the inspection report. Where a CA fails to take appropriate action in response to the inspection report, the accreditation authority may:

- indicate the irregularities, but allow the CA to continue operations until the next programmed inspection; or
- allow the CA to continue operations for a maximum of ninety days pending correction of any problems prior to revocation; or
- revoke the CA's certificate.

Where the accreditation authority fails to take any action, the PMA may revoke the CA's cross-certificate with the CCF.

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

2.7.6 Communication of results

CAs cross-certified with the CCF must provide the PMA with a copy of the results of the compliance inspection. These results will not be made public unless required by law. The method and detail of notification of inspection results to CAs cross-certified with the CA must be defined within the cross-certification agreement between the two parties.

2.8 Confidentiality of Information

Certificates and CRLs, and personal or corporate information appearing on them and in public directories are not considered sensitive, (sensitive in accordance with the Government Security Policy). All other personal or corporate information held by a CA or an LRA (e.g., registration and revocation information, logged events, correspondence between the Subscriber and the CA or LRA, etc.) is considered sensitive and must not be disclosed without the prior consent of the Subscriber, unless required by law.

The Digital Signature private key of each Subscriber is to be held only by the Subscriber and must be kept confidential by them. Any disclosure by the Subscriber is at the Subscriber's own risk.

Inspection information is to be considered sensitive and must not be disclosed to anyone for any purpose other than inspection purposes or where required by law.

Information pertaining to the CA's management of a Subscriber's Digital Signature certificate may only be disclosed to the Subscriber, the Sponsor or where required by law.

Any requests for the disclosure of information must be signed and delivered to the CA.

Any disclosure of information is subject to the requirements of the *Privacy Act*, the *Access to Information Act*, other relevant legislation and any applicable Government of Canada policy.

2.9 Intellectual property rights

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

Distinguished names must be unique for all End-entities of a CA. For each End-Entity additional numbers or letters may be appended to the `commonName` to ensure the RDN's uniqueness. The Unique Identifiers capability to differentiate Subscribers with identical names will not be supported.

3.1.5 Name claim dispute resolution procedure

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

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

3.1.6 Recognition, authentication and roles of trademarks

The use of trademarks will be reserved to registered trademark holders.

3.1.7 Method to prove possession of private key

No stipulation.

3.1.8 Authentication of organization identity

The identification of a prospective Subscriber may range from on line submission to face to face authentication in person.

3.1.9 Authentication of individual identity

The identification of a prospective Subscriber may range from on line submission to face to face authentication in person.

3.1.10 Authentication of devices or applications

No stipulation.

3.2 Authentication for routine rekey

A request for rekey may only be made by the Entity in whose name the keys have been issued. The CA must authenticate all requests for rekey, and the subsequent response must be authenticated by the Entity. This may be done by an on-line method in accordance with PKIX Part 3 – Certificate Management Protocol. An Entity requesting rekey may authenticate the request for rekey using its valid Digital Signature key pair. Where one of the keys has expired the request for rekey must be authenticated in the same manner as the initial registration.

3.3 Authentication for rekey after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, a CA must authenticate a rekey in the same manner as for initial registration. The CA must verify any change in the information contained in a certificate or the LRA authorized to act on behalf of that CA before that certificate is issued.

3.4 Authentication of revocation request

A CA, or an LRA acting on its behalf, must authenticate a request for revocation of a certificate. A CA must establish and make publicly available the process by which it addresses such requests and the means by which it will establish the validity of the request.

Requests for revocation of certificates must be logged.

4. OPERATIONAL REQUIREMENTS

4.1 Application for a certificate

The procedures and requirements for Certificate application will be established and published in the CPS or a publicly available document.

4.1.1 Application for a cross-certificate

The CCF will identify all procedures and requirements with respect to an application for a Cross-Certificate in its cross-certification procedures.

A CA requesting cross-certification through the CCF must ensure that each application be accompanied by:

- its Certificate Policy;
- an external audit inspection report validating the assurance level stated in the CP;
- the public verification key generated by the CA.

An application for a cross-certificate does not oblige the CCF to issue a cross-certificate.

4.2 Certificate issuance

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

4.3 Certificate acceptance

A CA must ensure that an Entity acknowledges acceptance of a certificate. For a device or application the individual or organization responsible for the device or application may do this acknowledgement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A CA may, but is not required to, revoke certificates. Where a CA adopts a policy of revoking certificates, it should follow the requirements as set out in the Basic Assurance policy.

Where a CA is cross-certified with the CCF, the CCF must revoke a cross-certificate:

- when any of the information in the certificate changes;
- upon suspected or known compromise of the private key;
- upon suspected or known compromise of the media holding the private key.

The PMA, in its discretion, may revoke a cross-certificate when a CA fails to comply with obligations set out in this CP, any agreement or any applicable law.

4.4.2 Who can request revocation

No stipulation for End-Entity certificates.

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

- the CA on whose behalf the cross-certificate was issued;
- the personnel operating the CCF;
- the PMA.

4.4.3 Procedure for revocation request

No stipulation.

4.4.4 Revocation request grace period

No stipulation.

4.4.5 Circumstances for suspension

The GOC PKI does not currently support certificate suspension.

4.4.6 Who can request suspension

Not applicable.

4.4.7 Procedure for suspension request

Not applicable.

4.4.8 Limits on suspension period

Not applicable.

4.4.9 CRL issuance frequency

No stipulation.

4.4.10 CRL checking requirements

No stipulation.

4.4.11 On-line revocation/status checking availability

The GOC PKI does not currently support on-line revocation/status checking.

4.4.12 On-line revocation checking requirements

Not applicable.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

Not applicable.

4.4.15 Special requirements re: key compromise

In the event of the compromise, or suspected compromise, of a CA signing key, the CA must immediately notify all CAs to whom it has issued cross-certificates and the PMA.

There is no requirement for any other Entity to notify the CA in the event of the compromise or suspected compromise of its private key.

4.5 System Security Audit Procedures

4.5.1 Types of event recorded

No stipulation.

4.5.2 Frequency of audit log processing

No stipulation.

4.5.3 Retention period for audit log

No stipulation.

4.5.4 Protection of audit log

No stipulation.

4.5.5 Audit log back-up procedures

No stipulation.

4.5.6 Audit collection system

No stipulation.

4.5.7 Notification to event causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records archival

No stipulation.

4.7 Key changeover

No stipulation.

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, and/or data are corrupted

No stipulation.

4.8.2 Entity public certificate is revoked

No stipulation.

4.8.2.1 Entity public certificate is downgraded

No stipulation.

4.8.3 Entity key is compromised

No stipulation.

4.8.4 Secure facility after a natural or other type of disaster

No stipulation.

4.9 CA termination

No stipulation.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY

5.1 Physical Controls

5.1.1 & 5.1.2 Site location, construction and physical access

The CA site must:

- satisfy at least the requirements for a Operations Zone; and
- be manually or electronically monitored for unauthorized intrusion.

If LRA workstations are employed, each LRA workstation must be located in an area that satisfies the controls required for a Reception Zone.

Where a PIN or password is recorded, it must be stored in a locked filing cabinet or container accessible only to designated personnel.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site back-up

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CA trusted roles

A CA may permit all duties for critical CA operations to be performed by one individual.

5.2.1.2 LRA trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.3 Personnel security controls

A CA must ensure that all personnel performing duties with respect to the operation of a CA or LRA must:

- be appointed in writing;
- be bound by contract or statute to the terms and conditions of the position they are to fill;
- have received comprehensive training with respect to the duties they are to perform;
- be bound by statute or contract not to disclose sensitive CA security-relevant information or Subscriber information; and
- not be assigned duties that may cause a conflict of interest with their CA or LRA duties.

5.3.1 Background, qualifications, experience, and clearance requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA must hold an ERC (Enhanced Reliability Check). A CA must ensure that all personnel who operate a LRA workstation for the purpose of on-line Entity management with the CA must hold an ERC (Enhanced Reliability Check).

5.3.2 Background check procedures

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

5.3.3 Training requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA or LRA must receive comprehensive training in:

- the CA/LRA security principles and mechanisms;
- all PKI software versions in use on the CA system;
- all PKI duties they are expected to perform; and
- disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

The requirements of 5.3.3 must be kept current to accommodate changes in the CA system. Refresher training must be conducted as required, and the CA must review these requirements at least once a year.

5.3.5 Job rotation

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA or LRA, a CA may suspend his or her access to the CA system.

5.3.7 Contracting personnel

CA must ensure that contractor access to the CA site is in accordance with 5.1.1.

5.3.8 Documentation supplied to personnel

A CA must make available to its CA and LRA personnel the certificate policies it supports, its CPS, and any specific statutes, policies or contracts relevant to their position.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

No stipulation.

6.1.2 Private key delivery to Entity

No stipulation.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to users

No stipulation.

6.1.5 Asymmetric key sizes

A CA must ensure that the key pairs for all PKI entities must be either 512 or 1024 bit RSA or DSA.

6.1.6 Public key parameters generation

A CA that utilises the DSA must generate parameters in accordance with FIPS 186.

6.1.7 Parameter quality checking

Not applicable.

6.1.8 Hardware/software key generation

No stipulation.

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

No stipulation.

6.2 Private key protection

The certificate holder must protect its private keys from disclosure.

6.2.1 Standards for crypto-module

Refer to 6.8.

6.2.2 Private key multi-person control

No stipulation.

6.2.3 Private key escrow

Digital Signature private keys must not be escrowed.

6.2.4 Private key back-up

No stipulation.

6.2.5 Private key archival

Refer to 4.6.

6.2.6 Private key entry into cryptographic module

No stipulation.

6.2.7 Method of activating private key

No stipulation.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

No stipulation.

6.3.2 Usage periods for the public and private keys

Keys may have validity periods of no more than one year if CRLs are not used and six years if CRLs are used.

6.4 Activation Data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

Computer Security Rating (CC Evaluation level) TBD.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Cryptographic module engineering controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number

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

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

`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, version 3(2)
`Serial Number:`	unique serial number for certificate

as well as the certificate extensions defined 7.1.2.

7.1.2 Certificate extensions

All Entity PKI software must correctly process the extensions identified in 4.2.1 and 4.2.2 of the PKIX certificate profile. The CPS must define the use of any extensions supported by the CA, its LRAs and End Entities.

The `certificatePolicies` field must be set as critical in all GOC PKI certificates.

7.1.3 Algorithm object Ids – CRL distribution points for difference assurance levels

The CA must use and End-entities must support, for signing and verification, the following algorithms:

- RSA1024 in accordance with PKCS#1 - [OID TBD];
- SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2) - [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Issuing Authority RSADSI].

Entities may use, for signing and verification, the following algorithms:

- RSA 512, RSA 1024, RSA 2048 in accordance with PKCS#1 - [OID TBD];
- DSA in accordance with DSS (FIPS PUB 186) and ANSI X9.30 (Part 1) - [OID TBD];
- MD5 in accordance with RFC 1321 - [OID TBD];
- SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2) - [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Issuing Authority RSADSI].

7.1.4 Name forms

No stipulation.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

A CA must ensure that the Policy OID is contained within the certificates it issues.

7.1.7 Usage of policy constraints extension

A CA must populate and mark as critical the `policyConstraints` extension.

7.1.8 Policy qualifiers syntax and semantics

A CA must populate the `policyQualifiers` extension with the URI of its CP. If the CA populates the `userNotice` extension, such text shall be limited to the text described in 2.1.1.

7.1.9 Processing semantics for the critical certificate policy extension

Critical extensions shall be interpreted as defined in PKIX.

7.2 CRL Profile

7.2.1 Version number

If implementing CRLs, the CA must issue X.509 version two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2 CRL and CRL entry extensions

If CRLs are implemented, they must conform to the requirements of the Basic Assurance policy.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

8.1.1 Items that can change without notification

None.

8.1.2 Changes with notification

Prior to making any changes to this certificate policy, the PMA will notify the CCF and all CAs that are directly cross-certified with the CCF.

8.1.2.1 List of items

All items in this certificate policy are subject to the notification requirement.

8.1.2.2 Notification mechanism

The PMA will notify, in writing, all CAs that are directly cross-certified with the CCF of any proposed changes to this certificate policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PMA may request CAs to notify their Subscribers of the proposed changes. The PMA will also post a notice of the proposal on the PMA World Wide Web site.

8.1.2.3 Comment period

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4 Mechanism to handle comments

Written and signed comments on proposed changes must be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the PMA.

8.1.2.5 Period for final change notice

The PMA will determine the period for final change notice.

8.1.2.6 Items whose change requires a new policy

If a policy change is determined by the PMA to warrant the issuance of a new policy, the PMA may assign a new Object Identifier (OID) for the modified policy.

8.2 Publication and notification procedures

An electronic copy of this document, digital signed by an authorized representative of the CA, is to be made available:

- at the PMA World Wide Web site, URL (TBD);
- via an e-mail request to [address to be supplied].

8.3 CPS approval procedures

A CA's accreditation into the GOC PKI must be in accordance with procedures specified by the PMA. Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.