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

CERTIFICATE POLICY

DIGITAL SIGNATURE

HIGH ASSURANCE LEVEL

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

id-gocpki-certpcy-digitalSignature-highAssurance ::=
id-gocpki-certpcy-sign-4

VERSION 3.02
APRIL 1999

TABLE OF CONTENTS

PART 1 – BACKGROUND

PART 2 – POLICY SPECIFICATION

PART 1 – BACKGROUND

1. INTRODUCTION

This document defines the Digital Signature certificate policy – high 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. Such availability may be affected by system maintenance, system repair or factors outside the control of the CA. The Government of Canada does not represent or warrant 100% availability offered under the GOCPKI.

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

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 ___________________.

This policy has been designed to be used in certain situations and identifies specific roles and responsibilities for CAs which issue this type of certificate and for Local Registration Authorities which must perform tasks that may be assigned to them by the CA. Subscribers and Relying Parties also have specific obligations which are outlined in this policy.

A CA may issue cross-certificates at this level of assurance and is obliged to inform Subscribers which applications are intended to be used with the GOC PKI system.

A CA must ensure that it associates itself and uses one Certificate and one CRL repository for this type of certificate. Certificates must be made available to Subscribers.

The use of high assurance level confidentiality keys is appropriate for the confidentiality of designated information that, if compromised, could cause extremely grave injury outside the national interest.

For this type of certificate, the Crown in right of Canada disclaims all liability for any use of this type of certificate other than uses permitted by the CA. The Crown in right of Canada limits its liability for permitted uses to $1,000,000 per instance of use.

Any disputes concerning key or certificate management under this policy are to be resolved by the Parties concerned using an appropriate dispute settlement mechanism (i.e. through negotiation, mediation or arbitration).

Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

A CA is required to maintain records or information logs in the manner described in this policy.

A CA should ensure that critical CA functions are performed by at least three individuals.

Digital signature keys must not be backed-up or otherwise stored. Keys may have a validity period as indicated in this policy. Confidentiality keys issued by a CA will be backed-up to protect against data loss or data corruption.

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 responsib le 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-highAssurance ::= {id-gocpki-certpcy-sign-4}

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, PKI personnel and (where permitted) other CAs with their signature verification keys;
- promulgating certificate status through CRLs; and
- ensuring adherence to this certificate policy.

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)

An LRA operating under this certificate policy is responsible for all duties assigned to it by the CA.

An LRA may perform duties on behalf of more than one CA, providing that in doing so it satisfies all the requirements of this CP.

1.3.3 Repositories

A CA must ensure that there is at least one certificate and CRL repository associated with it. This repository should be in the form of one or more directories that comply with the GOC X.500 standards profile.

A repository may or may not be under the control of a CA. Where a repository is not under the control of a CA, the CA must ensure that the terms and conditions of its association include, but are not limited to, the subjects of availability, access control, integrity of data, directory replication and directory chaining.

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 authorization 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

A Relying Party may be either a Subscriber of the GOC PKI or a Subscriber of a PKI which has signed a cross-certification agreement with the GOC PKI.

1.3.6 Policy applicability

This policy is suitable for the integrity and authentication of business transactions that if falsified could cause the loss of life, imprisonment, major financial loss, or require legal action for correction.

1.3.6.1 Approved and prohibited applications

A CA must advise Subscribers which applications are intended to be used with the PKI system.

Applications making use of high assurance certificates should undergo independent review to ensure that they, as a minimum, meet the following requirements:

- correctly establishes, transfers and uses the public and private keys;

- is capable of performing the appropriate certificate validity and verification checking; and
- reports 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 must make CRLs available to a Subscriber or Relying Party in accordance with 4.4. An Issuing CA must notify a Subscriber when a certificate bearing the Subscriber's DN is issued or revoked.

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

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

The CA must ensure that the Entity completes its initialization process immediately upon receipt of activation data.

2.1.1.4 Certificate revocation and renewal

The Issuing CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this CP and will be expressly stated in the Subscriber Agreement and any other applicable document outlining the terms and conditions of the certificate use. The CA must ensure that the key changeover procedures are in accordance with 4.7. The Issuing CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in 4.4.4 and 4.4.9. The address of the CRL must be defined in the certificate.

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)

A CA must ensure that all its LRAs comply with all the relevant provisions of this CP and the CA's CPS.

A CA is responsible through its LRA personnel to bring to the attention of Subscribers all relevant information pertaining to the rights and obligations of the CA, LRA and Subscriber contained in this CP, the Subscriber agreement, if applicable, and any other relevant document outlining the terms and conditions of use.

Records of all actions carried out in performance of LRA duties must identify the individual who performed the particular duty.

LRA Administrators must be individually accountable for actions performed on behalf of the CA. Individually accountable means that there must be evidence that attributes an action to the person performing the action.

2.1.2.1 Notification of certificate issuance and revocation

There is no requirement for an LRA to notify a Relying Party of the issuance or revocation of a certificate.

2.1.2.2 Accuracy of representations

When an LRA submits Subscriber information to a CA, it must certify to the CA that it has authenticated the identity of that Subscriber in accordance with 3 and 4.

2.1.2.3 Protection of LRA private keys

Each person performing LRA duties on-line through a remote administration application with the CA must ensure that his or her private keys are protected in accordance with 5 and 6.

2.1.2.4 Restrictions on LRA private key use

Private keys used by an LRA administrator to access and operate LRA Applications on-line with the CA must not be used for any other purpose.

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

Where a Subscriber suspects private key compromise, he or she must immediately notify the Issuing CA in a manner specified by that CA.

Where any other entity suspects private key compromise, they should immediately notify the Issuing CA.

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

Prior to using a certificate, a Relying Party must check the status of the certificate against the appropriate and current CRL in accordance with the requirements stated in 4.4.10. As part of this verification process the digital signature of the CRL must also be validated.

2.1.5 Repository obligations

The repository should be available for a high proportion of every 24-hour period. Certificates and CRLs must be available to Relying Parties in accordance with the requirements of 4.4.9.

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.

CAs and LRAs will ensure that their authentication and validation procedures are implemented as set forth in 3.

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 high level certificate or its associated public/private key pair, in excess of $1,000,000 per instance of use by a Subscriber or Relying Party.

Departments may establish their own liability limits above this recommended level 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

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

A dispute related to key and certificate management between departments should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved by the PMA or, where appropriate, through a mediator or arbitrator(s) appointed by the PMA.

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

Each CA must ensure that any agreement it enters into provides appropriate dispute resolution procedures.

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, 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 this 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 twelve months thereafter.

One of every five inspections must be done by an agency external to the department. The PMA, at its discretion, may request the Deputy Minister responsible for the CA to have a compliance inspection by an agency external to the department at any time.

The CA must certify annually to the PMA that they have at all times during the period in question complied with the requirements of this policy. The CA must also provide to the PMA reasons for which the CA has not complied with its CP and state any periods of non-compliance.

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 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 thirty days pending correction of any problems prior to revocation; or

- downgrade the assurance level of any cross-certificates; or
- revoke the CA's certificate.

Where the accreditation authority fails to take any action, the PMA may :

- downgrade the assurance level of the cross-certificate with the CCF; or
- 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

Each Entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate `subjectName` field and in accordance with PKIX Part 1. Each Entity may use an alternative name via the `SubjectAlternateName` field, which must also be in accordance with PKIX Part 1. 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 contents of each certificate `Subject` and `Issuer` name fields must have an association with the authenticated name of the Entity. In the case of individuals the Relative Distinguished Name (RDN) should be a combination of first name, surname, and optionally initials. This RDN may also include an organizational position or role. In the case of other entities the RDN will reflect the authenticated legal name of the Entity.

Where a certificate refers to a role or position, the certificate must also contain the identity of the person who holds that role or position.

A certificate issued for a device or application must include within the DN the name of the person or organization responsible for that device or application.

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

Prior to the issuance of a verification certificate, the Issuing CA and End-Entity will confirm their respective identities through the use of a shared secret.

The key transfer protocol described in PKIX Certificate Management Protocol is suitable for this requirement.

3.1.8 Authentication of organization identity

These certificates are not intended for use by organizations. Where the technology does not permit the independent generation of Digital Signature and Confidentiality key pairs, the Digital Signature key pair shall not be used.

3.1.9 Authentication of individual identity

An application for an individual to be a Subscriber may be made by the individual or by another person or organization authorized to act on behalf of the prospective Subscriber.

In addition to the identification and authentication described below, the prospective Subscriber must personally present him or herself to the CA or LRA for authentication prior to token initialization.

Identification and authentication of the individual must be through one of the following means:

- the CA or LRA will compare the identity of the individual with two pieces of identification (notarized copies or originals). At least one of these must be government identification containing a photograph; or
- if the department has previously established the identity of an individual using a process that satisfies the CA, and there have been no changes in the information presented, then the CA or LRA and the individual may utilize this privately shared information.

The CA or LRA must keep a record of the type and details of identification used.

3.1.10 Authentication of devices or applications

An application for a device or application to be an End-Entity may be made by an individual or organization to which the device's or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant must follow 3.1.8 or 3.1.9 as if that individual or organization was applying for the certificate on its own behalf.

The CA or LRA must also verify the identity of the individual or organization making the application and its authority to receive the keys for that device or application.

The CA or LRA must keep a record of the type and details of identification used.

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. All requests for rekey must be authenticated by the CA, 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. Any change in the information contained in a certificate must be verified by the CA 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

A CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in the CPS or a publicly available document. Bulk applications on behalf of End-Entities are permitted to be made only by persons authorized to make such applications.

A CA must ensure that each application be accompanied by:

- proof of the End-Entity's identity;
- proof of authorization for any requested certificate attributes;
- in the case of employees, an acknowledgement, or in the case of other subscribers, a signed agreement, of the applicable terms and conditions governing their use of the certificate;
- a public verification key generated by the End-Entity.

An application for a certificate does not oblige a CA to issue a certificate.

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 this acknowledgement may be done by the individual or organization responsible for the device or application.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate must be revoked:

- 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 CA in its discretion may revoke a certificate when an Entity fails to comply with obligations set out in this CP, the CPS, any agreement or any applicable law.

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

The revocation of a certificate may only be requested by:

- the Subscriber in whose name the certificate was issued;
- the individual or organization which made the application for the certificate on behalf of a device or application;
- the Sponsor;
- personnel of the Issuing CA;
- personnel of an LRA associated with the Issuing CA.

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

A CA must ensure that all procedures and requirements with respect to the revocation of a certificate are set out in the CPS or otherwise made publicly available. An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained. In the case where a certificate is revoked, full justification for the revocation must also be documented.

Where an Entity certificate is revoked, the revocation will be published in the appropriate CRL. Where a cross-certificate is revoked the revocation will be published in the ARL of the Issuing CA.

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 immediately upon receipt.

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

A CA must ensure that it issues an up to date CRL at least every four hours. A CA must also ensure that its CRL issuance is synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to Relying Parties. When a certificate is revoked due to key compromise the updated CRL must be issued immediately.

4.4.10 CRL checking requirements

A Relying Party must check the status of all certificates in the certificate validation chain against the current CRLs and ARLs prior to their use. A Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

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.

In the event of the compromise, or suspected compromise, of any other Entity's signing key, an Entity must notify the Issuing CA immediately.

A CA must ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.5 System Security Audit Procedures

4.5.1 Types of event recorded

A CA should record in audit log files all events relating to the security of the CA system. These include such events as:

- system start-up and shutdown;
- CA application start-up and shutdown;
- attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
- changes to CA details and/or keys;
- changes to certificate creation policies e.g., validity period;
- login and logoff attempts;
- unauthorized attempts at network access to the CA system;
- unauthorized attempts to access system files;
- generation of own and subordinate Entity keys;
- creation and revocation of certificates;
- attempts to initialize remove, enable, and disable Subscribers, and update and recover their keys;
- failed read-and-write operations on the certificate and CRL directory.

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

A CA should also collect and consolidate, either electronically or manually, security information not CA-system generated such as:

- physical access logs;
- system configuration changes and maintenance;
- personnel changes;
- discrepancy and compromise reports;
- records of the destruction of media containing key material, activation data, or personal Subscriber information.

A CA must ensure that the CPS indicates what information is 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.

4.5.2 Frequency of audit log processing

A CA must ensure that its audit logs are reviewed by CA personnel at least daily and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Supporting manual and electronic logs from the CA and LRA should be compared where any action is deemed suspicious.

Actions taken following these reviews must be documented.

4.5.3 Retention period for audit log

A CA must retain its audit logs onsite for at least two months and subsequently retain them in the manner described in 4.6.

4.5.4 Protection of audit log

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information must be protected from unauthorized viewing, modification and destruction.

4.5.5 Audit log back-up procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

4.5.6 Audit collection system

A CA must identify its audit collection systems in the CPS.

4.5.7 Notification to event causing subject

Where an event is logged by the audit collection system no notice need be given to the individual, organization, device or application which caused the event.

4.5.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA must ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

4.6 Records archival

Digital Signature certificates, Confidentiality private keys stored by the CA, and ARLs and CRLs generated by the CA, must be retained for at least one year after the expiration of the key material. This requirement does not include the back-up of private signature keys.

Audit information as detailed in 4.5, Subscriber agreements and any identification and authentication information should be retained for at least six years.

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

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

A CA should verify the integrity of the back-ups once every six months.

Material stored off-site must be periodically verified for data integrity.

In addition to the foregoing, information retained or backed up by a CA may be subject to the *National Archives Act*.

4.7 Key changeover

A Subscriber may only apply to renew his or her key pair within three months prior to the expiration of one of the keys, provided the previous certificate has not been revoked. A Subscriber, the CA, or the LRA may initiate this key changeover process. Automated key changeover is permitted. A CA must ensure that the details of this process are indicated in its CPS.

Subscribers without valid keys must be re-authenticated by the CA or LRA in the same manner as the initial registration.

Where a Subscriber's certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance.

Keys may not be renewed using an expired Digital Signature key.

4.8 Compromise and Disaster Recovery

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

A CA must establish business continuity 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, a CA must ensure any agreement with the repository provides that business continuity procedures be established and documented by the repository.

4.8.2 Entity public certificate is revoked

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

- the PMA;
- all CAs to whom it has issued cross-certificates;
- all of its LRAs;
- all Subscribers;
- all individuals or organizations who are responsible for a certificate used by a device or application.

The CA must also:

- publish the certificate serial number on an appropriate CRL;
- revoke all cross-certificates signed with the revoked Digital Signature certificate.

After addressing the factors that led to revocation, the CA may:

- generate a new CA signing key pair;
- re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the need for revocation of any other Entity's Digital Signature certificate see 4.4.

4.8.2.1 Entity public certificate is downgraded

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

- the PMA;
- all CAs to whom it has issued cross-certificates;
- all of its LRAs;
- all Subscribers;
- all individuals or organizations who are responsible for a certificate used by a device or application.

Prior to re-establishing cross-certification a CA must also:

- request revocation of cross-certificates issued to the CA;
- revoke all certificates signed with the higher assurance key;
- provide appropriate notice (see 4.8.2);
- generate a new CA signing key pair;
- re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the need for downgrade of any other Entity's Digital Signature certificate the CA or LRA must notify the Subscriber in a manner set out in its CPS and the subscriber agreement.

4.8.3 Entity key is compromised

In the event of the compromise of a CA's Digital Signature key, prior to re-certification within the GOC PKI, a CA must:

- request revocation of cross-certificates issued to the CA;
- revoke all certificates issued using that key;
- provide appropriate notice (see 4.8.2).

After addressing the factors that led to key compromise, the CA may:

- generate a new CA signing key pair;
- re-issue certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

In the event of the compromise, or suspected compromise, of any other Entity's Digital Signature key, the Entity must notify the Issuing CA immediately.

A CA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.8.4 Secure facility after a natural or other type of disaster

A CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the CA, a CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

4.9 CA termination

In the event that a CA ceases operation, it must notify its Subscribers immediately upon the termination of operations and arrange for the continued retention of the CA's keys and information. It must also notify all CA's with whom it is cross-certified.

In the event of a change in management of a CA's operations, the CA must notify all Entities for which it has issued certificates and CA's with whom it has cross-certified.

In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance the certificates issued by the CA whose operations are being transferred must be revoked through a CRL signed by that CA prior to the transfer.

The CA archives should be retained in the manner and for the time indicated in 4.6.

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 Security Zone;
- be manually or electronically monitored for unauthorized intrusion at all times;
- ensure unescorted access to the CA server is limited to those personnel identified on an access list;
- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and paper containing sensitive plain text information are stored in containers either listed in, or of equivalent strength to those listed in, the Security Equipment Guide.

In addition to the requirements of a CA, the CCF must satisfy at least the requirements for a High-Security Zone.

All LRA sites must be located in areas that satisfy the controls required for a Reception Zone.

If an LRA workstation is used for on-line Entity management with the CA, the workstation must be located in either:

- a Security Zone; or
- an Operations Zone while attended with all media security protected when unattended.

The CA will ensure the operation of the LRA site provides appropriate security protection of the cryptographic module, all system software and the LRA Administrator’s private key. The CA must conduct a threat and risk assessment. For example, the cryptographic module and the LRA Administrator’s private key could be stored in a secure container or safe.

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

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

The Subscriber’s hardware cryptomodule must be protected physically. This may be done through site protection or being kept with the Subscriber.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

A CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire prevention and protection

A CA must ensure that the CA system is protected with a fire suppression system.

5.1.6 Media storage

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

5.1.7 Waste disposal

All media used for the storage of information such as keys, activation data or CA files is to be sanitized or destroyed before released for disposal.

5.1.8 Off-site back-up

A CA must ensure that facilities used for off-site back-up, if any, have the same level of security as the primary CA site.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CA trusted roles

A CA must ensure 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 is to be limited to those actions for which they are required to perform in fulfilling their responsibilities.

A CA should provide for a minimum of three distinct PKI personnel roles, distinguishing between day-to-day operation of the CA system, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel. The division of responsibilities between the three roles should be as follows:

PKI Master User

- configuration and maintenance of the CA system hardware and software;
- commencement and cessation of CA services.

PKI Officer

- management of PKI Operators and other PKI Officers;
- configuring CA security policies;
- verification of audit logs;
- verification of CP and CPS compliance.

PKI Administrator

- management of the Subscriber initialization process;
- creation, renewal or revocation of certificates;
- distribution of tokens (where applicable).

An alternative division of responsibilities is permitted so long as it provides the same degree of resistance to insider attack.

Only those personnel responsible for the duties outlined for PKI Master User and System Administrator should have access to the software that controls the CA operation.

5.2.1.2 LRA trusted roles

A CA must ensure that LRA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

- acceptance of subscription, certificate change, certificate revocation and key recovery requests;
- verification of an applicant’s identity and authorizations;
- transmission of applicant information to the CA;
- provision of authorization codes for on-line key exchange and certificate creation.

A CA may permit all duties for LRA functions to be performed by one individual.

5.2.2 Number of persons required per task

A CA must ensure that no single individual may gain access to Subscriber private keys stored by the CA. At a minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any key recovery operation.

Multi-user control is also required for CA key generation as outlined in 6.2.2.

All other duties associated with CA roles may be performed by an individual operating alone. A CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

5.2.3 Identification and authentication for each role

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

- included in the access list for the CA site;
- included in the access list for physical access to the CA system;
- given a certificate for the performance of their CA role;
- given an account on the PKI system.

Each of these certificates and accounts (with the exception of CA signing certificates) must:

- be directly attributable to an individual;
- not be shared;

- be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

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 a Level II Security Clearance. 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) which must include fingerprint check and a credit 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

Each prospective certificate holder must generate its own Digital signature key pair using a PMA-approved algorithm.

6.1.2 Private key delivery to Entity

Not applicable.

6.1.3 Public key delivery to certificate issuer

The public verification key must be delivered to the CA either via an on-line transaction in accordance with the PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.

6.1.4 CA public key delivery to users

The CA public verification key must be delivered to the prospective certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PMA.

6.1.5 Asymmetric key sizes

A CA must ensure that the key pairs for all PKI entities must be 2048 bit RSA.

6.1.6 Public key parameters generation

A CA that utilizes 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

The generation of Digital Signature keys for all Entities must be generated in a hardware cryptographic module.

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

Keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment. CA signing keys are the only keys permitted to be used for signing certificates and CRLs.

The certificate `KeyUsage` field must be used in accordance with PKIX-1 Certificate and CRL Profile. One of the following `KeyUsage` values must be present in all certificates: `DigitalSignature` or `Non-Repudiation`.

One of the following additional values must be present in CA certificate-signing certificates: `Key Cert Sign` or `CRL Sign`.

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

There must be multiple person control for CA key generation operations. Two staff, performing duties associated with the roles of PKI Master User or PKI Officer positions, must participate or be present.

6.2.3 Private key escrow

Digital Signature private keys must not be escrowed.

6.2.4 Private key back-up

An Entity may optionally back-up its own Digital Signature private key. If so, the keys must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

6.2.5 Private key archival

Refer to 4.6.

6.2.6 Private key entry into cryptographic module

Not applicable.

6.2.7 Method of activating private key

The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

6.2.8 Method of deactivating private key

When keys are deactivated they must be cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity.

6.2.9 Method of destroying private key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. The method of over-writing must be approved by the PMA. Private key destruction procedures must be described in the CPS or other publicly available document.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The Issuing CA must retain all verification public keys.

6.3.2 Usage periods for the public and private keys

All keys (2048 bits) must have validity periods of no more than twenty years.

Suggested validity period:

- CA public verification key and certificate - twenty years;
- CA private signing key - eight years;
- End-Entity public verification key and certificate - twelve years;
- End-Entity private signing key - two years.

Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

6.4 Activation Data

6.4.1 Activation data generation and installation

Any activation data must be unique and unpredictable. 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, an Entity must have the capability to change its password at any time.

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 private keys of Entities must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Each CA server must include the following functionality:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities;
- object re-use or separation for CA random access memory;
- use of cryptography for session communication and database security;
- archival of CA and End-Entity history and audit data;
- audit of security related events;
- self-test of security related CA services;
- trusted path for identification of PKI roles and associated identities;
- recovery mechanisms for keys and the CA system;
- enforcement of domain integrity boundaries for security critical processes.

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

6.5.2 Computer security rating

Computer Security Rating (CC Evaluation level) TBD.

CSE, NSA or other accredited third party laboratory must evaluate the security critical elements of the CA. Such an evaluation must include system-level analysis.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The CA must use CA software that has been designed and developed either under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), or Information Systems Security Engineering Handbook.

The design and development process must provide sufficient documentation to support third party security evaluation of the CA components and be supported by:

- third party verification of process compliance;
- on-going Threat Risk Assessments to influence security safeguard design and minimize residual risk.

6.6.2 Security management controls

A formal configuration management methodology must be used for 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:

- originated from the software developer;

- has not been modified prior to installation; and
- is the version intended for use.

The CA must provide a mechanism to periodically verify the integrity of the software.

The CA must also have mechanisms and policies in place to control and monitor the configuration of the CA system.

Upon installation time, and at least once every 24 hours, the integrity of the CA system must be validated.

6.7 Network security controls

The CA server must be protected from attack through any open or general purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA.

A CA must ensure that its CPS defines those protocols and commands required for the operation of the CA.

6.8 Cryptographic module engineering controls

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 level 2 or otherwise verified to an equivalent level of functionality.

The LRA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

All other LRA cryptographic operations must be performed cryptographic modules rated at FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

End Entities must use a hardware cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

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:

- RSA 2048 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 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

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

7.1.5 Name constraints

`Subject` and `Issuer` DNs must comply with PKIX standards and be present in all certificates.

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

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

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

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.