Draft – For Discussion Only

Government of Canada Public Key Infrastructure

Cross-Certification Methodology and Criteria

Version: September 22, 1999

Table of Contents

FOREWORD

Objective

This document outlines the procedures and criteria for cross-certification with the Canadian Central Facility of the Government of Canada Public Key Infrastructure.

Background

In May 1999, Treasury Board Ministers approved the policy for Public Key Infrastructure Management in the Government of Canada. The policy defines the Government of Canada Public Key Infrastructure as a “public key infrastructure for use by Departments which operates in accordance with the standards, guidelines and directions of the Policy Management Authority”.

The Policy Management Authority comprises representatives of each federal department operating at least one Certification Authority that is part of the Government of Canada Public Key Infrastructure. Its membership also includes a representative of the Canadian Central Facility. The Policy Management Authority is responsible for the oversight and management of the Government of Canada Public Key Infrastructure.

The Policy Management Authority is also responsible for recommending, to the Secretary of the Treasury Board, the approval or rejection of requests for cross-certification. It is the authority for establishing procedures and standards both for the Canadian Central Facility and for Certification Authorities that are part of the Government of Canada Public Key Infrastructure. The policy for Public Key Infrastructure Management in the Government of Canada stipulates that if a departmental Certification Authority intends to issue, or have issued on its behalf, certificates outside the department, it must cross-certify with the Canadian Central Facility.

For cross-certifications internal to the federal community, the Government of Canada Public Key Infrastructure Management policy requires departments to be members of the Government of Canada Public Key Infrastructure, and to sign a cross-certification arrangement formally describing the terms and conditions of the cross-certification. Cross-certifications with the private sector or with certification authorities not part of the Government of Canada Public Key Infrastructure require the implementation of formal cross-certification arrangements between the Government of Canada and the external entity.

The Government of Canada Public Key Infrastructure Secretariat supports the Policy Management Authority and the Treasury Board Secretary in their respective responsibilities for the direction and management of the Government of Canada Public Key Infrastructure.

Intended Audience

This publication, which is issued under the authority of the Policy Management Authority, is intended for the use of federal information technology officials, Certification Authorities and public key infrastructure managers and personnel involved in cross-certification activities within the government and between government and external Certification Authorities.

These cross-certification guidelines should be read in conjunction with the Treasury Board policy for Public Key Infrastructure Management in the Government of Canada, particularly Appendices B and D, the Memorandum of Understanding, and Minimum Terms and Conditions required for Cross-Certification Arrangements, respectively. It is also important to consult federal Public Key Infrastructure Certificate Policies. Both these texts are published on the Internet at http://www.cio-dpi.gc.ca/pki/Documents/documents_e.html.

Readers can find further detail on the Government of Canada Public Key Infrastructure at http://www.cio-dpi.gc.ca/pki/home_e.html. Requests for information can also be directed to the Government of Canada Public Key Infrastructure Secretariat at pki-icp@tbs-sct.gc.ca.

Definitions

The following terms are used in these guidelines:

Canadian Central Facility: the Government of Canada Public Key Infrastructure's central Certification Authority.

Certification Authority: a person or organizational unit within a department responsible for:

(a) the operation of an authority trusted by one or more users to issue and manage public key certificates and certificate revocation lists; or

(b) the management of:

(i) any arrangement under which a department contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and

(ii) policies and procedures within the department for the management of public key certificates issued on its behalf.

A Certification Authority within a department remains at all times responsible and accountable for the management of public key certificates that it issues or arranges to be issued on behalf of the department.

Certificate Policy: a named set of rules that indicates the applicability of a public key certificate to a particular community and/or class of application with common security requirements. It indicates whether the public key certificate is suitable for a particular application or purpose. A Certification Authority may adopt more than one certificate policy.

Certification Practice Statement: a statement of the practices that a Certification Authority employs in issuing public key certificates. It is a comprehensive description of such details as the precise implementation of service offerings and procedures of public key certificate life-cycle management. The Certificate Practice Statement is more detailed than the certificate policies supported by the Certification Authority.

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

Cross-Certification: the process undertaken by Certification Authorities to establish a trust relationship. When two Certification Authorities are cross-certified, they agree to trust and rely on each other's public key certificates and keys as if they had issued them themselves. The Certification Authorities exchange cross-certificates and enable users from one Certification Authority to interact electronically and securely with users from another.

Digital Signature: the result of a transformation of a message by means of a cryptographic system using keys so 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: any person employed by a department and being issued a certificate in the capacity of employee and, for greater certainty, does not include external subscribers.

External subscriber: any person not an employee or one issued a certificate in the capacity of an employee. Includes a member of the public, a client of, or supplier to, the government and, for greater certainty, includes a service-provider such as a consultant under contract to the government who is being issued a certificate in the capacity of service-provider.

Key*:* a sequence of symbols that controls digital signature and encryption processes.

Public Key Certificate: the public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it.

Public Key Infrastructure: the entire set of policies, processes, server platforms, software, and work stations used for (the purpose of) administering certificates and keys.

Repository: a system for storing and accessing certificates or other information relevant to certificates. The Government of Canada Public Key Infrastructure repository is an X.500 directory.

Standard: a level of attainment regarded as a measure of adequacy; requirements and guidelines approved for government-wide use. (Operational standards form part of the Treasury Board Manual; technical standards are produced by Policy Management Authority).

Subscriber: a person whose public key is certified in a certificate. In the Government of Canada Public Key Infrastructure, subscribers are employees and external subscribers.

PART ONE: OVERVIEW

Government of Canada Public Key Infrastructure – An Introduction

A Public Key Infrastructure supports data encryption and digital signature applications, using a system of mathematical formulae to produce public and private keys. A trusted third party, known as a Certification Authority, associates the public and private key pairs with a specific person or entity. The Certification Authority identifies the person or entity who is to receive a key pair, issues keys, revokes them when required, and provides notice of revocations.

The Certification Authority issues digital certificates – the electronic document or record associating a particular key pair to a specific person or entity, thus verifying the identity of the key holder. In the Government of Canada Public Key Infrastructure, certificates operate at four levels of assurance: rudimentary, basic, medium and high. Federal departments determine the appropriate level of assurance necessary, depending on their business, security and legal requirements. As the need for assurance escalates, so too does the effort taken by the Certification Authority to confirm the identity of the certificate holder.

Depending on a number of factors, including the level of assurance required, Certification Authorities issue different types of certificates. Rules governing the issuance of specific classes of certificates are captured in Certificate Policies, which serve as the cornerstone of trust in a public key certificate and form the basis for cross-certification. Certification Authorities cross-certifying with each other establish a trust relationship in which each recognizes one or more Certificate Policies of the other. In the Government of Canada Public Key Infrastructure, these trust relationships – or cross-certifications – are established through the Canadian Central Facility, whether such relationships exist between federal bodies governed by the Treasury Board's Public Key Infrastructure management policy, or with external Certification Authorities.

The proposed federal cross-certification methodology contains four phases, with up to 14 discrete steps. The following is an executive overview of the proposed methodology, which is fully detailed in Part Two.

Proposed Cross-Certification Process – A Summary

Phase I: Initiation

Phase I covers the initiation of the cross-certification process. It comprises three steps:

- The initial request in which the candidate prepares and submits the required information to cross-certify with the Government of Canada Public Key Infrastructure.
- A request review by the Government of Canada Public Key Infrastructure Secretariat, to establish the candidate's suitability for cross-certification.
- The Government of Canada Policy Management Authority's (PMA) decision on whether to continue the process of cross-certification.

Phase II: Examination

Phase II covers the examination phase of the process. Its four steps include:

- An examination of the candidate's Certificate Policies to establish their degree of harmonization with the Certificate Policies of the Government of Canada.
- A test bed trial to identify and resolve potential incompatibilities between the Certification Authority technologies of the Government of Canada Public Key Infrastructure and the

candidate, using a Test Bed Certification Authority to minimize the risk to cross-certified Certification Authorities already in production mode.

- A system survey to confirm that the technical details of the respective Certification Authorities are available for production mode cross-certification.
- An evaluation of the candidate's information technology security and policy compliance, to:
  - conduct a security analysis to ensure that, as part of an information technology system, the Candidate Certification Authority provides an appropriate level of trust.
  - establish if the technical, physical, procedural and personnel policies of the Candidate Certification Authority meet the assurance requirements of its Certificate Policies.
  - determine if the Candidate Certification Authority's actual performance meets the standards established in its Certificate Policies and other Certification Authority operational documents.

Phase III: Arrangement

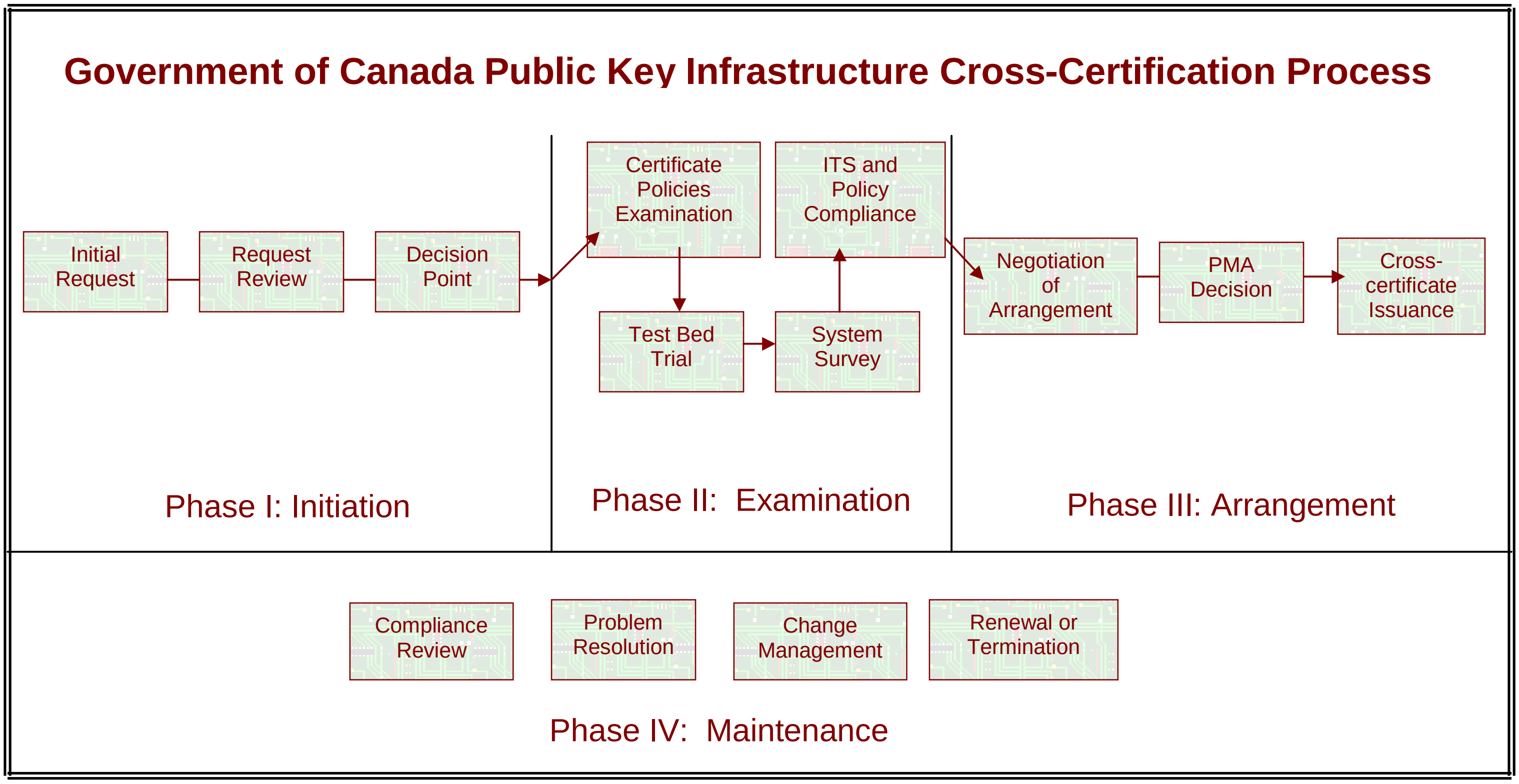
Phase III relates to the formal documentation of the terms and conditions under which a candidate becomes a member of the Government of Canada Public Key Infrastructure and it cross-certified by the Canadian Central Facility. Its three steps encompass:

- The negotiation of the terms and conditions governing the cross-certification arrangement.
- The Policy Management Authority decision on whether to enter into the cross-certification arrangement with the candidate.
- The initiation of the process allowing the Canadian Central Facility and the Candidate Certification Authority to issue cross-certificates.

Phase IV: Maintenance

Phase IV concerns the maintenance of the trust established in the cross-certification arrangement. It provides mechanisms both for managing the relationship between cross-certified Certification Authorities and for terminating the arrangement if either party contravenes its terms and conditions. The elements of this phase are not sequential and apply as circumstances warrant. It comprises four possible steps:

- A review to determine if the cross-certified Certification Authority is operating in compliance with its stated policies and procedures.
- A problem resolution process to report and correct problems either party may encounter over the period of the cross-certification arrangement.
- A process to manage changes to the public key infrastructure associated with a particular cross-certification arrangement, and to decide on actions to take in response to implementing such changes.
- A procedure for renewing or terminating a cross-certification arrangement.



Government of Canada Public Key Infrastructure Cross-Certification Process

PART TWO: METHODOLOGY

Government of Canada Public Key Infrastructure – Cross-Certification Process

A request to cross-certify with the Government of Canada Public Key Infrastructure triggers a multi-phase process designed to achieve a mutually reliable trust relationship.

Phase I – Initiation

- Request by Candidate Certification Authority to cross-certify with the Government of Canada Public Key Infrastructure.
- Initial review of policy, technical and legal issues.
- Policy Management Authority decision to reject request or proceed to next phase.

Phase I, Step 1: Initial Request
Purpose

To prepare and submit the required information to cross-certify with the Government of Canada Public Key Infrastructure.

Step 1, Initial Request: Activities

1. The Candidate Certification Authority contacts the Government of Canada Public Key Infrastructure Secretariat to initiate the process to allow it to cross-certify with the Government of Canada Public Key Infrastructure. (If the candidate organization is external to the federal government, it must identify a sponsoring department which is a Government of Canada Public Key Infrastructure member.)

2. A Government of Canada Public Key Infrastructure Secretariat desk officer, who is now the point of contact for the candidate, provides the candidate the following Government of Canada Public Key Infrastructure documents:

   (a) Security Policy Index (Annex 10)
   (b) Security Procedures Index (Annex 11)
   (c) Information Technology Security checklist (Annex 9)
   (d) Compliance Inspection Checklist (Annex 12)
   (e) System Survey (Annex 7)

   If required, the desk officer will also provide (e) a non-disclosure agreement.

3. The desk officer provides, and asks the candidate to complete, a Request for Cross-Certification (Annex 1). The Candidate Certification Authority (or its sponsor) can seek the desk officer's assistance in completing or revising the Request, which seeks the following information:

   (a) Candidate Certification Authority identifying information, its departmental sponsor (if any), and contacts;
   (b) Reason for requesting cross-certification;
   (c) A description of the Candidate Certification Authority's proposed technical operational environment and configuration, and clients;
   (d) A checklist for developing a profile of the candidate, concerning its operation. The checklist asks for particulars on the candidate's:

      i. Certificate Policies, their number and nature
      ii. Security policies and procedures
      iii. Most recent compliance inspection results
      iv. PKI technology and product version

v. Procedures for key recovery (if any)
vi. Directory technologies
vii. Signature and encryption algorithms
viii. Certificate verification process (such as use of Certification Revocation Lists)
ix. Applicable sovereign immunity laws (if any)
x. Level of assurance sought.

If the Candidate Certification Authority is an organization not governed by the scope of the Policy for Public Key Infrastructure Management in the Government of Canada (an external Candidate Certification Authority), it may be asked to provide:

(e) evidence of the current legal status of the organization operating the Certification Authority, and
(f) evidence of the financial capacity of the organization operating the Certification Authority(such as bonds, letters of credit, insurance demonstrating the organization's ability to meet the financial responsibilities associate with operating a Certification Authority.

4. The Candidate Certification Authority submits the completed Request for Cross-Certification form (which has been signed by the appropriate senior officials) to the desk officer. The form must be accompanied by the candidate's Certificate Policy and completed Test Bed System Survey. The candidate identifies a principal point of contact. The candidate or its sponsor can seek the desk officer's advice on completing or revising the Request for Cross-Certification form.

5. An External Candidate Certification Authority must submit a written statement from its sponsoring department, stating its reasons for endorsing the cross-certification request.

6. External Candidate Certification Authorities must submit an executed non-disclosure agreement (Annex 2).

7. The desk officer reviews the submitted form and other supporting documentation to ensure it has been completed properly. If there are any errors or omissions in the form or documentation, the desk officer will return them to the candidate for revision.

Standard Activities	**Additional Activities – External CCAs**	**Phase I, Step 1: Initial Request – Activities**
1.		CCA initiates process.
2.		Desk officer provides background documentation.
3.		Desk officer provides Request for Cross-Certification form.
	3.a	External CCA provides information on legal and financial status (if necessary).
4.		CCA submits completed Request for Cross-Certification, Certification Policy and CA Test Bed System Survey.
5.		External CCA submits sponsoring department statement.
6.		External CCA submits non-disclosure agreement.
7.		Desk officer reviews submission and other documentation.

Phase I, Step 2: Request Review

Purpose

To establish the Candidate’s suitability for cross-certification.

Step 2, Request Review: Activities

1. The desk officer, having received the completed Request for Cross-Certification and all supporting documentation, conducts an initial review of the Request, using criteria specified in Part III.

2. If necessary, the desk officer seeks additional information from the candidate or sponsoring department to assist the Policy Management Authority in its review of the request.

3. The desk officer prepares a Request Review Report (Annex 3), which contains the recommendation to the Policy Management Authority whether to proceed to the next step in the cross-certification process.

4. The desk officer submits the Request Review Report to the Policy Management Authority for its decision.

Phase I, Step 2: Application Review - Activities	
1.	Desk officer undertakes initial review of Request for Cross-Certification.
2.	Desk officer seeks additional information from CCA (if necessary).
3.	Desk officer prepares Request Review Report recommending either to proceed ,or terminate the process.
4.	Desk officer submits Request Review Report to PMA.

Phase I, Step 3: Decision Point

Purpose

To decide whether to continue the cross-certification request process.

Step 3, Decision Point: Activities

1. The Policy Management Authority reviews the Request Review Report. It may seek clarification or additional information from the desk officer, the candidate, or the sponsoring department, as is appropriate.

2. Within 60 days of the desk officer receiving the Request for Cross-Certification and all supporting documentation, the Policy Management Authority renders its decision on whether to proceed with the Request.

3. The Policy Management Authority chair signs the decision, and provides it to the desk officer.

4. The desk officer communicates the Policy Management Authority decision to the candidate, ensuring that the point of contact understands that a decision to proceed with the cross-certification process in no way implies eventual acceptance of the request.

If the decision is to proceed with the cross-certification process:

5. The Policy Management Authority Secretariat creates a cross-certification team .

6. The desk officer provides the candidate point of contact a copy of the cross-certification team’s Terms of Reference (Annex 4).

7. The desk officer informs Government of Canada Public Key Infrastructure members of the Request for Cross-Certification to determine whether they wish to cross-certify with the candidate if the Policy Management Authority ultimately recommends the acceptance of the Request.

8. As it is received, the desk officer provides the Canadian Central Facility information on departmental Certification Authorities wishing to cross-certify with the candidate, so that the Canadian Central Facility can take it into account during the Test Bed Trial, Step 5.

9. The cross-certification team leader and the candidate point of contact organize an initial meeting between the cross-certification team and Candidate Certification Authority personnel to allow the team to outline the cross-certification process and answer questions from the candidate.

	Phase I, Step 3: Decision Point - Activities
1.	PMA reviews Request Review Report.
2.	PMA renders decision on whether to proceed with Request for Cross-Certification.
3.	PMA chair signs decision and informs desk officer.
4.	Desk officer informs CCA of decision.
If decision is to proceed …	
5.	PMA creates cross-certification team.
6.	Desk officer provides the CCA the cross-certification team’s Terms of Reference.
7.	Desk officer informs GOC PKI members of the Request..
8.	Desk officer informs CCF of GOC PKI members wishing to cross-certify with candidate if request accepted.
9.	Cross-certification team leader and CCA contact organize information meeting.

PHASE II- EXAMINATION

- Examination of Certificate Policies
- Test Bed Trial
- System Survey (Production Testing)
- Evaluation of Candidate Certification Authority's Information Technology Security and Policy Compliance

Phase II, Step 4: Examination of Certificate Policies

Purpose

To examine the candidate's Certificate Policies and to establish their degree of harmonization with the Certificate Policies of the Government of Canada.

Step 4, Examination of Certificate Policies: Activities

1. The candidate contact identifies which of the candidate's Certificate Policies are to be considered for cross-certification with the Government of Canada Public Key Infrastructure.

2. The cross-certification team determines the type of document and the type of certificate (whether digital signature or confidentiality) covered by the Certificate Policy submitted by the candidate. This process is illustrated in the Certificate Policy Mapping Guidelines in Part III.

3. The cross-certification team maps the candidate's Certificate Policy(ies) to the Government of Canada Public Key Infrastructure Certificate Policy(ies), using the Certificate Policy Mapping Sheets (Annex 5).

4. The cross-certification team prepares a Certificate Policy Mapping Report (Annex 6) and provides a copy of the Mapping Report to the desk officer. Any section of the Certificate Policy Mapping Sheets marked critical must be accompanied by a statement of the associated risk the identified situation poses to the Government of Canada.

5. The Certificate Policy Mapping Report recommends one of the following:

   (a) proceed to the next step without conditions;
   (b) proceed to the next step, with acceptance by candidate to conditions;
   (c) terminate process.

6. The desk officer informs the Policy Management Authority of the Certificate Policy Mapping Report recommendation.

7. The Policy Management Authority reviews the CP Mapping Report recommendation and decides whether to proceed to the next step or terminate the process.

8. The desk officer informs the Candidate Certificate Authority's contact of the outcome of the Policy Management Authority review of the CP Mapping Report recommendation.

Phase II, Step 4: Examination of Certificate Policies – Activities

1.	CCA identifies Certificate Policies to be cross-certified with GOC PKI.
2.	The cross-certification team determines the CP type submitted by the CCA.
3.	The cross-certification team maps the CCA's CP(s) to the GOC PKI CP(s).
4.	The cross-certification team completes the Certificate Mapping Report and provides a copy to the desk officer.
5.	The Certificate Mapping Report makes one of three recommendations: - proceed without conditions - proceed with conditions - terminate process
6.	The desk officer informs the PMA of the Report's recommendation.
7.	The PMA reviews the recommendation and decides whether to proceed to the next step or terminate the process.
8.	The desk officer informs the candidate of the outcome of the PMA review and decision.

If the decision is to proceed, then the process moves to:

Phase II, Step 5: Test Bed Trial

Purpose

To identify and resolve potential incompatibilities between the Certification Authority technologies of the Government of Canada Public Key Infrastructure and the candidate, using a Test Bed Certification Authority and thus minimizing the risk to cross-certified Certification Authorities already in production mode.

Step 5, Test Bed Trial: Activities

1. The Policy Management Authority designates a Government of Canada Public Key Infrastructure Test Bed Certification Authority, which may be located either at the Canadian Central Facility or another facility contracted for that purpose.

2. The cross-certification team reviews the candidate's completed Test Bed System Survey (Annex 7) which provides information on the technical configuration of the candidate to permit it and the Government of Canada Public Key Infrastructure Test Bed Certification Authority to "inter-operate" at a technical level . (The candidate's Certification Authority may be either its intended production or test bed Certification Authority. If it is the candidate's test bed Certification Authority, it must accurately represent the properties and specifications of the candidate's production Public Key Infrastructure for the purposes of cross-certification.)

3. The cross-certification team provides the candidate's contact the current Government of Canada Public Key Infrastructure Test Bed Certification Authority System Survey results, and thus its technical configuration data.

4. Having shared their respective technical data, the Candidate Certification Authority and the Government of Canada Public Key Infrastructure undertake a test cross-certification. As this process is technology-dependent, it is not described here; however, it must demonstrate both the:

   (a) successful exchange of Certification Authority certificates
   (b) the ability of each party to validate the other's certificates.

5. The cross-certification team documents the findings of the trial in the Test Bed Trial Report (Annex 8) and provides a copy to the desk officer.

6. The Test Bed Trial Report recommends one of the following:

   (a) proceed to the next step without conditions;
   (b) proceed to the next step, with acceptance by candidate of conditions;
   (c) terminate process.

7. The desk officer provides the Report to the Policy Management Authority.

8. The Policy Management Authority reviews the Test Bed Trial Report recommendation and decides whether to proceed to the next step or terminate the process.

9. The desk officer informs the Candidate Certificate Authority's contact of the Policy Management Authority decision on the Test Bed Trial Report recommendation.

Phase II, Step 5: Test Bed Trial – Activities

1.	PMA designates a GOC PKI Test Bed CA.
2.	The cross-certification team reviews the candidate's System Survey.
3.	The cross-certification team provides the candidate the System Survey for the GOC PKI CA.
4.	The candidate and the GOC PKI undertake a test cross-certification.
5.	The cross-certification team prepares a Test Bed Trial Report and provides a copy to the desk officer.
6.	The Test Bed Trial Report makes one of three recommendations: - proceed without conditions - proceed with conditions - terminate process
7.	The desk officer provides the Report's recommendation to the PMA.
8.	The PMA reviews the recommendation and decides whether to proceed to the next step or terminate the process.
9.	The desk officer informs the candidate of the outcome of the PMA review and decision.

If the decision is to proceed, then the process moves on to:

Phase II, Step 6: System Survey (Production Testing)

Purpose

To confirm that the technical details of the respective Certification Authorities are available for production mode cross-certification.

Step 6, System Survey: Activities

1. The candidate point of contact completes a System Survey for the candidate's Certification Authority to be connected permanently to the Canadian Central Facility.

2. The contact returns the completed Survey to the cross-certification team.

3. The cross-certification team concurrently provides the contact the Canadian Central Facility's current System Survey results so the candidate has the necessary technical configuration data, and is aware of the Facility's production environment. Follow-ups between the respective parties for clarification or further information will take place as required.

	Phase II, Step 6: System Survey (Production Testing) – Activities
1.	The candidate contact completes a System Survey for the CA, which will be connected permanently to the Canadian Central Facility.
2.	The contact returns the completed Survey to the cross-certification team.
3.	The cross-certification team provides the candidate contact the Canadian Central Facility's latest System Survey.

Phase II, Step 7: Evaluation of Candidate's Information Technology Security and Policy Compliance

Purpose

(a) To conduct a security analysis to ensure that, as part of an information technology system, the Candidate Certification Authority provides an appropriate level of trust.
(b) To establish if the technical, physical, procedural and personnel policies of the Candidate Certification Authority meet the assurance requirements of its Certificate Policies.
(c) To determine if the Candidate Certification Authority's actual performance meets the standards established in its Certificate Policies and other Certification Authority operational documents.

Step 7, Evaluation of Candidate's Information Technology Security and Policy Compliance: Activities

1. The candidate completes the Information Technology Security Evaluation checklist (Annex 9) provided in Phase I. The candidate may use the Government of Canada Public Key Infrastructure Security Policy Index (Annex 10) and the Government of Canada Public Key Infrastructure Certification Authority Security Procedures Index (Annex 11), provided by the desk officer in Phase I, as templates to assist in completing the checklist if it has not already developed such documentation.

2. The candidate uses the Information Technology Security Evaluation checklist and the Compliance Inspection Checklist (Annex 12), provided by the desk officer in Phase I, as the baseline criteria for evaluating its Information Technology Security and Policy Compliance results.

3. The candidate conducts, or has a qualified Information Technology Security evaluator conduct on its behalf, an Information Technology Security evaluation.

4. If the candidate's and the Government of Canada Public Key Infrastructure's respective Information Technology Security evaluation criteria and processes are similar, the candidate provides the cross-certification team a comparison between its Information Technology Security criteria and the Information Technology Security checklist (Annex 9).

5. The candidate conducts, or has a qualified Compliance Inspector conduct on its behalf, a Compliance Inspection which reviews all relevant documents, including the candidate's Certificate Policy(ies), and Certificate Practice Statement(s). Although not strictly bound to the Model Government of Canada Public Key Infrastructure Compliance checklist, the candidate must certify a specific Certification Authority assurance level and provide the cross-certification team, for analytical purposes, the framework it used in conducting the compliance inspection.

6. The candidate provides the cross-certification team a comparison between its compliance evaluation criteria and the Compliance Inspection checklist, if it has already conducted a compliance inspection.

7. The candidate's contact completes an Information Technology Security and Policy Compliance Certificate (Annex 13).

8. A senior official of the Candidate Certification Authority signs the Information Technology Security and Policy Compliance Certificate, attesting on behalf of the candidate that:

   (a) the candidate has completed, or has had completed on its behalf by a qualified inspector, an inspection and evaluation according to the Information Technology Security and Compliance Inspection checklists; or an Information Technology Security evaluation and policy compliance inspection which accords substantially with those checklists.

   (b) the candidate's information technology security system is certified (or approved) for, and operates at a level of assurance of _____________ (as described in the candidate organization's Certificate Policy(ies) and Certificate Policy Statement(s)).

   (c) the candidate's technical, physical, procedural and personnel security policies and practices both comply with the requirements of its Certificate Policy(ies) and Certificate Policy Statement(s) and fully perform in accordance with the standards established in its Certificate Policy(ies) and Certificate Policy Statement(s).

9. In exceptional circumstances, and on the direction of the Policy Management Authority, the cross-certification team leader may request that the team be permitted to visit, or have someone visit on its behalf, the candidate's Certification Authority facilities, its Local Registration Authorities' (LRA) sites, or specific Subscribers, to ensure that the candidate complies fully with its Certification Authority procedures.

10. The cross-certification team analyzes the candidate's signed and completed Information Technology Security and Policy Compliance Certificate, and its Certificate Practice Statement(s) to confirm that the candidate has met the checklist security requirements. If necessary, the cross-certification team will request additional information or clarification from the candidate.

11. The cross-certification team documents its findings in the Information Technology Security and Policy Compliance Evaluation Report (Annex 14) and provides a copy to the desk officer.

12. The Information Technology Security and Policy Compliance Report recommends one of the following:

    (a) proceed to the next step without conditions;
    (b) proceed to the next step, with acceptance by candidate of conditions;
    (c) terminate process.

13. The Policy Management Authority reviews the Information Technology Security and Policy Compliance Report recommendation and decides whether to proceed to the next step or terminate the process.

14. The desk officer informs the candidate of the Policy Management Authority review and decision.

Phase II, Step 7: Evaluation of ITS and Policy Compliance – Activities	
1.	The candidate completes the ITS Evaluation checklist.
2.	The candidate uses the ITS Evaluation and Compliance Inspection checklists as baseline criteria for evaluations.
3.	The candidate undertakes an ITS evaluation.
4.	The candidate provides the cross-certification team a comparison of its ITS criteria and the GOC PKI ITS checklist.
5.	The candidate undertakes a Compliance Inspection, certifying a specific assurance level and providing the cross-certification team the framework it used for the compliance inspection.
6.	If it has already conducted a compliance inspection, the candidate provides the cross-certification team a comparison between its compliance evaluation criteria and the Compliance Inspection checklist.
7.	The candidate's contact completes an ITS and Policy Compliance certificate (Annex 13).
8.	A senior officer of the candidate organization signs the ITS and Policy Compliance Certificate, attesting: - that the candidate has undertaken ITS and Policy Compliance inspections; - that the candidate's ITS system is certified and operates at a specific assurance level; and, - that the candidate's technical, physical, procedural and personnel security policies and practices comply, and fully perform in accordance with, the candidate's Certificate Policy(ies) and Certificate Policy Statement(s).
9.	The cross-certification team may undertake a visit to the candidate's CA facilities, its LRA sites, or specific Subscribers, to ensure full compliance in the candidate's CA procedures.
10.	The cross-certification team reviews the signed ITS and Policy Compliance Certificate and CPS to confirm that the candidate has met the checklist security requirements.
11.	The cross-certification team documents its findings in an ITS and Policy Compliance Evaluation Report and provides a copy to the desk officer.
12.	The ITS and Policy Compliance Report makes one of three recommendations: - proceed without condition - proceed with conditions - terminate process
13.	The PMA reviews the recommendation and decides whether to proceed to the next step or terminate the process.
14.	The desk officer informs the candidate of the PMA decision.

If the decision is to proceed, then the process moves on to:

PHASE III – ARRANGEMENT

- Negotiation of Arrangement
- Decision Point
- Initialization

Phase III, Step 8: Negotiation of Arrangement

Purpose

To negotiate the terms and conditions of the cross-certification arrangement.

Step 8, Negotiation of Arrangement: Activities

1. In consultation with legal counsel, the cross-certification team determines which type of document is appropriate to serve as the prototype for a cross-certification agreement. The arrangement may be either a Cross-Certification Arrangement (Annex 15), the Government of Canada Public Key Infrastructure Memorandum of Understanding (Annex 16), or some other formal arrangement, such as a treaty with a foreign government.

2. Process for External Cross-Certification Arrangement

   2.1 The cross-certification team provides a review copy of the appropriate draft arrangement to the candidate's contact.

   2.2 The cross-certification team provides any additional information or clarification required by the candidate.

   2.3 The cross-certification team and the candidate negotiate text for the proposed arrangement. The team must ensure that the candidate understands that the negotiations in no way implies eventual acceptance of the Candidate Request for Cross-Certification, nor do they commit the Government of Canada Public Key Infrastructure to the issuance of any cross-certificates.

   2.4 Using the Negotiation Report (Annex 17), the cross-certification team details any differences between the document chosen as the basis for the arrangement and the negotiated arrangement.

3. Process for Interdepartmental Government of Canada Public Key Infrastructure Memorandum of Understanding

   3.1 The cross-certification team provides a review copy of the Memorandum of Understanding to the candidate's contact.

   3.2 The cross-certification team provides any additional information or clarification required by the candidate

4. Common Activity: Negotiation

   4.1 The cross-certification team may review any relevant documentation, such as subscriber or service provider agreements, related to the Candidate operation.

Phase III, Step 8: Negotiation of Arrangement – Activities		
1.	Cross-certification team determines appropriate type of arrangement for cross-certification.	
2.	External Cross-Certification	
	2.1	Cross-certification team provides the candidate a copy of the appropriate draft arrangement.
	2.2	Cross-certification team provides additional information or clarification.
	2.3	Cross-certification team and candidate personnel negotiate text.
	2.4	Cross-certification team details differences between negotiated arrangement and prototype arrangement.
3.	GOC PKI Memorandum of Understanding	
	3.1	Cross-certification team provides the candidate a copy of the GOC PKI MOU.
	3.2	Cross-certification team provides additional information or clarification.
4.	Cross-certification team reviews relevant documentation	

Phase III, Step 9: Policy Management Authority Decision

Purpose

To decide whether to enter into cross-certification arrangement with candidate.

Step 9, Policy Management Authority Decision: Activities

1. The cross-certification team prepares a Consolidated Evaluation Report (Annex 18) which details the findings of the CP Mapping, Information Technology Security and Policy Compliance, and Negotiation Reports. The Report also contains the team's recommendation on whether the Government of Canada Public Key Infrastructure should cross-certify with the candidate.

2. The Consolidated Evaluation Report recommends one of the following:

    (a) proceed to the next step without conditions;
    (b) proceed to the next step, with acceptance by candidate of conditions;
    (c) terminate process.

2. The desk officer forwards the Consolidated Evaluation Report and its recommendation to the Policy Management Authority, seeking a decision on the candidate's request for cross-certification.

3. The Policy Management Authority reviews the Consolidated Evaluation Report and recommendation; it may also review other cross-certification team reports (Negotiation, CP Mapping, Test Bed Trial, Information Technology Security and Policy Compliance Reports), as well as ask the team for a presentation on the request for cross-certification.

4. Based on its review of the Consolidated Report and any of the other reports noted above, the Policy Management Authority prepares its response to the request for cross-certification, and forwards its recommendation to the Secretary of the Treasury Board, who recommends to the President.

5. The Policy Management Authority decision advises the Secretary to recommend one of three possible courses of action to the President:

    (a) cross-certify;
    (b) cross-certify only with candidate's acceptance of conditions;
    (c) reject the cross-certification request.

6. By means of a decision letter, the desk officer informs the candidate's point of contact of the President's decision.

7. If the decision letter recommends conditional acceptance of the cross-certification request, the desk officer asks the candidate point of contact to provide a written response within 20 days of the date of the decision letter.

If the decision is to proceed, then:

8. The cross-certification team is responsible for repeating any step(s) in the process necessitated by a recommendation for conditional acceptance. The Policy Management Authority must be consulted again to approve resolution of major issues.

9. Following the resolution of all issues identified in the original letter of decision, the desk officer generates a second letter of decision for the signature of the Policy Management Authority Chair. The letter indicates whether the cross-certification will proceed; the desk officer forwards the letter to the candidate contact.

10. If the decision is to proceed, appropriate representatives of the Crown and the Candidate Certification Authority sign the appropriate arrangement (either external Certification Authority arrangement, Government of Canada Public Key Infrastructure Memorandum of Understanding, or treaty).

12. Following the signing of the cross-certification arrangement, the desk officer and the candidate contact determine an appropriate start date, which is at least five days subsequent to the decision, to allow the Government of Canada Public Key Infrastructure Secretariat to communicate the decision to departmental Certification Authorities.

	Phase III, Step 9: Policy Management Authority Decision – Activities
1.	Cross-certification team prepares the Consolidated Evaluation Report containing recommendation on cross-certification request.
2.	The Consolidated Evaluation Report makes one of three recommendations: - proceed without condition - proceed with conditions - terminate process.
3.	Desk officer forwards the Consolidated Evaluation Report and recommendation to PMA.
4.	PMA reviews the Consolidated Evaluation Report and recommendation, as well as any of the various cross-certification process reports it deems necessary.
5.	PMA forwards its recommendation on the cross-certification request to the TB Secretary, for the consideration of the TB President.
6.	PMA decision advises the TBS Secretary and ultimately the TB President either to : - cross-certify, - cross-certify with CCA acceptance of conditions, or - reject cross-certification request.
7.	Desk officer issues a decision letter informing the CCA contact of the President's decision.
8.	The desk officer informs the contact that the candidate's written response to a conditional acceptance must be received no later than 20 days from the date of the President's decision.
9.	The cross-certification team undertakes any necessary repetition of steps in the process.
10.	If necessary, desk officer issues a second letter of decision signed by the PMA chair, indicating acceptance or rejection of cross-certification request.
11.	If the decision is to accept, representatives of both parties sign the appropriate cross-certification agreement.
12.	Desk officer and candidate contact determine an appropriate start date for the arrangement.

Phase III, Step 10: Issuance of Cross-Certificates

Purpose

To initiate the process allowing the Canadian Central Facility and the Candidate Certification Authority to issue cross-certificates.

Step 10, Issuance of Cross-Certificates: Activities

1. The cross-certification team provides the candidate's completed System Survey (from Step 6) to the Canadian Central Facility.

2. The Canadian Central Facility provides a completed System Survey for its Certification Authority to the candidate's point of contact.

3. Following a satisfactory review of the technical data provided by both parties, the two Certification Authorities issues cross-certificates. As the precise process is technology-dependent, it will not be described here; however, both parties must be able to:

   (a) successfully exchange Certification Authority certificates; and
   (b) recognize or validate the other's certificate directories.

4. The Canadian Central Facility informs the desk officer when the cross-certificates are issued.

5. The desk officer informs the Policy Management Authority and the members of the Government of Canada Public Key Infrastructure of the new cross-certification.

Phase III, Step 10: Issuance of Cross-Certificates – Activities	
1.	The cross-certification team provides the CCA's completed System Survey to the CCF.
2.	The CCF provides a completed System Survey for its CA to the CCA.
3.	The CAs issue cross-certificates.
4.	The CCF informs the desk officer of the cross-certification
5.	The desk officer informs the PMA and GOC PKI members of the new cross-certification

PHASE IV - MAINTENANCE

It is important to ensure that, once in place and for its duration, the cross-certification arrangement continues to maintain a level of trust between the two parties. Each cross-certification is governed by the arrangement entered into in Phase III. For example, the Government of Canada Public Key Infrastructure Memorandum of Understanding governs the relationship between departmental Certification Authorities and the Canadian Central Facility. The federal policy on Public Key Infrastructure Management in the Government of Canada and Policy Management Authority decisions also govern the relationship.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified Certification Authorities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions. The elements of this phase are not sequential, they will apply as circumstances warrant.

Should the Government of Canada Public Key Infrastructure Secretariat, the Canadian Central Facility or the Policy Management Authority become aware of any information that creates any doubt that there has been a failure:

(a) in the integrity of the Affiliated Certification Authority’s information technology security, or
(b) in the Affiliated Certification Authority’s compliance with its stated Certificate Policy or Certificate Practice Statement,

and such failure may adversely affect the security of the Government of Canada Public Key Infrastructure, the Chair of the Policy Management Authority may, at his or her discretion, instruct the Canadian Central Facility to revoke immediately the cross-certificate of the Affiliated Certification Authority. The Canadian Central Facility does so, informing the desk officer responsible for relations with the Affiliated Certification Authority of the revocation. The desk officer then informs the Affiliated Certification Authority and departmental Certification Authorities of the revocation.

Phase IV, Step 11: Compliance Review

Purpose

To determine if the Affiliated Certification Authority is operating in compliance with its stated polices and practices.

Step 11, Compliance Review: Activities

1. The desk officer requests the Affiliated Certification Authority to provide the Government of Canada Public Key Infrastructure Secretariat an Information Technology Security and Policy Compliance Certificate for a mutually agreed-upon period following the date of the initial cross-certification. Although this period may coincide with the review period specified in the arrangement, it is not required to.

2. When the desk officer receives the Information Technology and Policy Compliance Certificate for the compliance review period, her or she establishes a Compliance Review Team to manage relations with the Affiliated Certification Authority. While the desk officer may not head the Compliance Review Team, he or she remains responsible for liaison between the Compliance Review Team and the Affiliated Certification Authority.

3. The Compliance Review Team reviews the Information Technology Security and Policy Compliance Certificate, as well as any Problem or Change Management Reports and any other relevant documentation, to determine if there are any issues warranting particular attention.

4. In exceptional circumstances, and on the direction of the Policy Management Authority, the compliance review team leader may request that the team be permitted to visit, or have someone visit on its behalf, the Affiliated Certification Authority's facilities, its Local Registration Authorities (LRA) sites or specific Subscribers to ensure that there is full compliance in all the Affiliated Certification Authority's procedures.

5. The compliance review team prepares a Compliance Review Report (Annex 19) and provides a copy to the desk officer. The Compliance Review Report will:

   (a) indicate any deficiencies and suggest corrective action, but recommend that the Affiliated Certification Authority continues to be cross-certified at its current assurance level;
   (b) recommend renewal, but further recommend that the Canadian Central Facility downgrade the assurance level of the cross-certificate;
   (c) recommend that the Canadian Central Facility terminate the cross-certification.

6. The desk officer forwards the Compliance Review Report to the Policy Management Authority for review and decision within 30 days of the Report's receipt. If the report's recommendation is to terminate the arrangement, downgrade its status or continue with conditions, the Affiliate Certification Authority may initiate a Problem Resolution Report.

7. The desk officer informs the Canadian Central Facility and the Affiliated Certification Authority of the Policy Management Authority decision.

8. If the Policy Management Authority so directs, the Canadian Central Facility takes the appropriate actions to revoke the existing cross-certificate and, if required, issues a new cross-certificate.

9. The Canadian Central Facility informs the desk officer of the cross-certificate revocation and when, if applicable, it issues a new cross-certificate.

10. If, during the course of the Government of Canada Public Key Infrastructure Compliance Review, the team notes a deficiency which can be rectified by immediate corrective action, the team will inform the point of contact of the deficiency.

11. If the deficiencies cannot be corrected immediately, the desk officer advises the contact of an appropriate length of time for the Affiliated Certification Authority to rectify them. The contact informs the desk officer of any action the Affiliated Certification Authority has taken or expects to take in response to deficiencies identified in the Compliance Review Report.

	Phase IV, Step 11: Compliance Review – Activities
1.	Affiliated CA provides the GOC PKI Secretariat a report on ITS and Policy Compliance.
2.	Desk officer establishes a Compliance Review Team.
3.	Compliance Review Team reviews the review report as well as any Problem or Change Management Reports.
4.	The Compliance Review Team leader may request the Team be allowed to visit the Affiliated CA's facilities, its LRA sites or specific subscribers to ensure there is full compliance in the Affiliated CA's procedures.
5.	The team provides the desk officer a copy of its Compliance Review report, recommending one of three possible courses: ▪ indicate any deficiencies, suggest corrective action, but recommend that Affiliated CA continues to be cross-certified at its current assurance level; ▪ recommend renewal, but recommend the CCF downgrade the certificate's assurance level; ▪ recommend the CCF terminate the cross-certification.
6.	The desk officer forwards the Compliance Review Report to the PMA for review and decision within 30 days.
7.	The desk officer informs the CCF and the Affiliated Certification Authority of the PMA decision.
8.	If the PMA directs, the CCF revokes the existing cross-certificate. If required, the CCF issues a new certificate.
9.	The CCF informs the desk officer of the revocation and, if applicable, the issuance of a new cross-certificate.
10.	If during its review, the Compliance Review Team notes a deficiency which can be rectified immediately, the teams informs the Affiliate CA contact.
11.	If deficiencies cannot be correctly immediately, the desk officer advises the contact of the length of time the Affiliated CA has to make the corrections. The point of contact informs the desk officer of Affiliated CA actions to respond to deficiencies.

Phase IV, Step 12: Problem Resolution

Purpose

To report and correct problems the parties may encounter over the effective period of the cross-certification arrangement.

Step 12, Problem Resolution: Activities

1. Either party to the cross-certification arrangement may initiate this step by submitting a Problem Resolution Report (Annex 20) to the appropriate desk officer.

2. The desk officer authenticates the information in the Problem Resolution Report through discussions with the parties, and reviews of relevant documents, previous concerns and their resolution to determine any precedents.

3. The desk officer attempts to resolve the problem expeditiously, in collaboration with the cross-certification signatories.

4. If the desk officer cannot resolve the situation without delay, he or she documents it in the Problem Resolution Report, and provides copies to the Policy Management Authority and the cross-certification signatories. The problem is then handled in accordance with the terms and conditions of the cross-certification arrangement. In the case of departmental Certification Authorities, the Policy Management Authority may have to resolve the problem.

5. The desk officer documents all outcomes in the Problem Resolution Report.

	Phase IV, Step 12: Problem Resolution – Activities
1.	Either signatories to the cross-certification arrangement submits a Problem Resolution Report to the desk officer.
2.	The desk officer authenticates the information in the Problem Resolution Report.
3.	The desk officer, working with the cross-certification signatories, attempts to solve the problem expeditiously.
4.	If the desk officer cannot resolve the problem expeditiously, it is documented in the Problem Resolution Report, copies of which are provided to the PMA and the cross-certification signatories.
5.	The desk officer documents all outcomes in the Problem Resolution Report.

Phase IV, Step 13: Change Management

Purpose

To manage changes to the Public Key Infrastructure associated with a particular cross-certification arrangement. and to decide what actions to take as a result of implementing such changes.

Step 13, Change Management: Activities

1. Either party to the cross-certification arrangement may initiate this step by submitting a Change Management Report (Annex 21) to the appropriate desk officer.

2. The desk officer authenticates the information in the Change Management Report through discussions with the parties, and reviews of relevant documents, previous requests for changes and their resolution, to ascertain if there are any precedents.

3. The desk officer completes the appropriate section of the Change Management Report for review and consideration by the Policy Management Authority. The Report advises one of three possible actions:

   (a) unconditional acceptance of the requested change(s);
   (b) conditional acceptance, with follow-up required (the change is accepted but the next Compliance Review must pay particular attention to the change implementation);
   (c) the change is found to be unacceptable.

4. The Policy Management Authority reviews the Change Management Report and makes its decision, which is shared with the signatories to the cross-certification arrangement.

5. Should one of the parties implement a change that the Policy Management Authority has deemed unacceptable, such implementation may cause the Policy Management Authority to terminate the cross-certification arrangement or downgrade the assurance level.

6. If either the Canadian Central Facility or the Affiliated Certification Authority are dissatisfied with the Policy Management Authority decision, they must resolve the matter in accordance with provisions contained in the cross-certification arrangement.

7. The desk officer documents all outcomes in the Change Management Report and provides a copy to the Canadian Central Facility.

Phase IV, Step 13: Change Management – Activities	
1.	Either party to the cross-certification arrangement submits a Change Management Report to the desk officer.
2.	The desk officer authenticates the information in the Change Management Report.
3.	The desk officer completes the Change Management Report and forwards it to the PMA. The Report advises: ▪ unconditional acceptance of the requested change ▪ conditional acceptance of the change, with follow-up required ▪ the change is unacceptable
4.	PMA reviews the Report and comes to a decision.
5.	If one of the parties implements a change that has been deemed unacceptable, the PMA may terminate the cross-certification arrangement or downgrade the assurance level.
6.	If either the CCF or the Affiliated CA are dissatisfied with the PMA decision, they must resolve the matter according to provisions in the cross-certification arrangement.
7.	The desk officer documents all outcomes in the Change Management Report and provides a copy to the Canadian Central Facility.

Phase IV, Step 14: Renewal or Termination

Purpose

To decide whether to renew or terminate an existing cross-certification arrangement, and to specify the process for either renewal or termination.

Step 14, Renewal or Termination: Activities

The Government of Canada Public Key Infrastructure Secretariat serves as the repository for signed cross-certification arrangements. Whether in the form of an external cross-certification arrangement or the Government of Canada Public Key Infrastructure Memorandum of Understanding, any arrangement will last for the period specified in the arrangement.

A. Common Process

1. The desk officer provides the Policy Management Authority with a Renewal/Terminal Report (Annex 22) so the Policy Management Authority may make a determination on any renewal, termination or withdrawal request. The Report will contain:

   (a) a summary of all relevant issues and information from various documents, including:

   (i) the most recent Compliance Review Report;
   (ii) all Problem Resolution Reports since the arrangement was signed or last renewed;
   (iii) all Change Management Reports since the arrangement was signed or last renewed.

   (b) a recommendation to accept the request or, if appropriate, enter into negotiations to revise the cross-certification arrangement.

B. Renewal of Existing Arrangement with an External Certification Authority

1. The desk officer notifies the Policy Management Authority 180 days before the expiry date of any cross-certification arrangement, to allow the Policy Management Authority time to consider whether to renew the arrangement.

2. The desk officer contacts the other party to the arrangement to ascertain whether there is interest in renewing the arrangement, and to seek any information the party may wish the Policy Management Authority to consider in its deliberations.

3. The Policy Management Authority reviews the Renewal/Termination Report in light of the criteria described in Part III of the Guidelines.

4. The Policy Management Authority decides either to:

   (a) recommend to the Secretary of the Treasury Board (who recommends to the President) to renew the arrangement, for a specified period of time, with no changes;
   (b) enter into negotiations to revise the cross-certification arrangement and, depending on the outcome of the negotiations, subsequently to recommend to the Secretary of the Treasury Board (who recommends to the President) to enter into the arrangement.

5. If the Policy Management Authority recommends that the arrangement be renewed with no changes, the desk officer informs the other party, initiating the activities outlined in Phase II. Once those activities are completed, the desk officer prepares both a recommendation to the Secretary of the Treasury Board (for recommendation to the President), and a new arrangement for the signatures of both parties.

6. If the Policy Management Authority recommends the negotiation of a new arrangement, the desk officer informs the other party in writing. If the other party wishes to proceed, then Phases II and III will apply.

7. If the other party declines the Policy Management Authority recommendation, the arrangement will expire according to the provisions of the existing cross-certification arrangement.

C. External Certification Authority Request for Termination of Arrangement

1. Any party to an external cross-certification arrangement may submit a termination request at any time during the life of the arrangement. The request must include the reason(s) for seeking termination, and the desired termination date.

2. The desk officer, in consultation with the Canadian Central Facility and the Affiliated Certification Authority’s point of contact, determines a mutually agreeable termination date. The Canadian Central Facility and the external Certification Authority carry out the appropriate termination procedures.

3. The Canadian Central Facility notifies the desk officer on the completion of all termination procedures and the revocation of cross-certificates.

B. Government of Canada Public Key Infrastructure Member Withdrawal from the Government of Canada Public Key Infrastructure

1. At any time during the period of the arrangement, a departmental Certification Authority may contact the desk officer to request withdrawal from the Government of Canada Public Key Infrastructure. In accordance with the Government of Canada Public Key Infrastructure Memorandum of Understanding, the request must include the reason(s) for seeking termination and the desired termination date.

2. The Policy Management Authority specifies the terms and conditions for withdrawal from the Government of Canada Public Key Infrastructure, and notifies the desk officer.

3. The desk officer informs the “withdrawing” member of the Policy Management Authority terms and conditions for withdrawal.

4. Prior to the agreed-upon termination date, both the Canadian Central Facility and the withdrawing member carry out the appropriate termination procedures. The Canadian Central Facility notifies the desk officer following the completion of all termination procedures and the revocation of cross-certificates.

5. The desk officer informs all departmental Certification Authorities of the withdrawal.

C. Departmental Certification Authorities and Removal from the Government of Canada Public Key Infrastructure

1. Pursuant to the Government of Canada Public Key Infrastructure Memorandum of Understanding, the Policy Management Authority may remove a departmental Certification Authority from the Government of Canada Public Key Infrastructure. The desk officer notifies the member in writing of the Policy Management Authority action, noting the reason(s) for removal and the termination date, as stipulated in the Memorandum of Understanding.

2. The Policy Management Authority applies the criteria in Part III in making the decision to remove a member from the Government of Canada Public Key Infrastructure.

Phase IV, Step 14:Renewal or Termination – Activities

A. Common Process

The desk officer provides the PMA a Renewal/Termination Report, containing:

(a) a summary of all relevant issues and information

(b) a recommendation to accept the request, or to enter into negotiations to revise the cross-certification arrangement.

B. Renewal of Existing Arrangement with External Certification Authority

1. 180 days before the expiry of a cross-certification arrangement, the desk officer informs the PMA.
2. The desk officer contacts the other signatory to determine if the party wishes to renew the arrangement.
3. The PMA uses the criteria in Part III to review the Renewal/Termination Report.
4. The PMA decides either to:
   (a) recommend the renewal of the arrangement, for a specified period, with no changes.
   (b) enter into negotiations to revise the arrangement
5. If the PMA recommends renewal with no changes, the desk officer informs the other signatory, initiating Phase II activities. Once the activities are completed, the desk officer prepares a recommendation for the TBS Secretary and a new arrangement for both parties to sign.
6. If the PMA recommends negotiating a new arrangement, the desk officer informs the other party in writing. If that party wishes to proceed, Parts II and III apply.
7. If the other party declines the PMA recommendation, the arrangement expires.

C. External Certification Authority Request for Termination of Arrangement

1. Any signatory to an external cross-certification arrangement may request the termination of the arrangement, specifying the reasons for seeking termination and the desired termination date.
2. The desk officer, the CCF and the Affiliated CA determine a mutually agreeable termination date. The CCF and the Affiliated CA carry out appropriate termination procedures.
3. The CCF notifies the desk officer of the completion of the termination procedures and the revocation of cross-certificates.

D. GOC PKI Member Withdrawal from GOC PKI

1. A departmental CA may request to withdraw from the GOC PKI at any time, stating the reason(s) for seeking termination and the desired termination date.
2. The PMA specifies the terms and conditions for withdrawal, and notifies the desk officer.
3. The desk officer informs the withdrawing member of the PMA terms and conditions for withdrawal.
4. The CCF and the withdrawing member undertake the termination procedures.
5. The desk officer informs all departmental CAs of the withdrawal.

E. Departmental CAs and Removal from the GOC PKI

1. The desk officer notifies the member CA of a PMA decision to remove the member from the GOC PKI, stating the reason(s) for removal and the termination date.
2. The PMA uses the criteria in Part III in deciding to remove a member from the GOC PKI.

PART THREE: CRITERIA

Text to follow.

PART FOUR: CROSS-CERTIFICATION ANNEXES

Annex 1	Phase 1, Step 1	Request for Cross-Certification
Annex 2	Phase 1, Step 1	Non-Disclosure Agreement
Annex 3	Phase 1, Step 2	Request Review Report
Annex 4	Phase 1, Step 3	Cross-Certification Team - Terms of Reference
Annex 5	Phase 2, Step 4	CP Mapping Sheets
Annex 6	Phase 2, Step 4	CP Mapping Report
Annex 7	Phase 2, Step 5	System Survey Questionnaire
Annex 8	Phase 2, Step 5	Test Bed Trial Report
Annex 9	Phase 2, Step 7	Information Technology Security Checklist
Annex 10	Phase 2, Step 7	Security Policy Index
Annex 11	Phase 2, Step 7	Security Procedures Index
Annex 12	Phase 2, Step 7	Compliance Inspection Checklist
Annex 13	Phase 2, Step 7	ITS and Policy Compliance Certificate
Annex 14	Phase 2, Step 7	ITS and Policy Compliance Evaluation Report
Annex 15	Phase 3, Step 8	Cross-Certification Arrangement
Annex 16	Phase 3, Step 8	GOC PKI Memorandum of Understanding
Annex 17	Phase 3, Step 8	Negotiation Report
Annex 18	Phase 3, Step 9	Consolidated Evaluation Report
Annex 19	Phase 4, Step 11	Compliance Review Report
Annex 20	Phase 4, Step 12	Problem Resolution Report
Annex 21	Phase 4, Step 13	Change Management Report
Annex 22	Phase 4, Step 14	Renewal/Termination Report

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 1 - REQUEST FOR CROSS-CERTIFICATION

Section 1 Candidate Certification Authority ("Candidate")

(a) Name of Candidate
(b) Name of Organization(s) which operates Candidate
(c) Name of Individual(s) to serve as Candidate's Point of Contact
(d) Address
(e) Telephone
(f) Fax
(g) E-Mail address

Section 2 Department(s) serving as Candidate's Sponsor ("Sponsor")

(a) Name(s) of Department(s)
(b) Name(s) of Individual(s) to serve as Sponsor's Point of Contact
(c) Address
(d) Telephone
(e) Fax
(f) E-Mail address

Explanatory Note: Points of Contact, in consultation with the Candidate's policy, operations, technical and legal personnel, are to represent their Candidate, as required, at relevant stages of the cross-certification process.

Section 3 - Technology

The Candidate must indicate:

(a) Technology product employed (including version number);
(b) Signature and encryption algorithms supported;
(c) Directory technologies employed;
(d) Certificate verification process employed;
(e) Level of assurance sought;
(f) Existence, if any, of key recovery.

Section 4 - Documentation

Before any **Request for Cross-certification** can be considered complete, the Candidate must submit the following documentation:

(a) A letter from a Department[1] in the Government of Canada indicating that department's sponsorship of the Candidate.
(b) A document containing the reasons why the Government of Canada should enter into a cross-certification arrangement with the Candidate, and a list of the specific departments with which the Candidate wishes to cross-certify.
(c) A copy of the Candidate's Certificate Policy[2].

[1] Department means a department within the meaning of the Government of Canada Certificate Policies Document.
[2] There may be one or more Certificate Policies submitted.

(d) A statement of security assessment.

(e) A compliance inspection report indicating the results of any inspection of the Candidate within the preceding 12 months.

(f) A completed Testbed System Survey.

(g) A signed undertaking not to disclose any security-related information revealed for the purposes of facilitating cross-certification.

(h) A list of all Certification Authorities to which the Candidate has issued cross-certificates.

(i) A statement disclosing any laws concerning sovereign immunity that may apply to the Candidate or any organization that controls, directly or indirectly, the Candidate.

(j) If the organization operating the Candidate is a corporate entity, a copy of documents indicating current standing in the jurisdiction of incorporation and legal status.

(k) Evidence of financial standing.

Date:

Signature(s) of senior official(s) of the organization that operates the Candidate CA

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 2 - NON-DISCLOSURE AGREEMENT[3]

This Agreement made

Between:

HER MAJESTY THE QUEEN IN RIGHT OF CANADA
as represented by the President off the
Treasury Board of Canada
(hereinafter called "the Government of Canada")
Party of the First Part

and

XYZ
(hereinafter called "X")
Party of the Second Part

WHEREAS the Government of Canada is interested in entering into a cross-certification arrangement with X;

AND WHEREAS the Government of Canada understands that in order for X to make its decision to cross-certify, X will need to review existing confidential information in written, electronic, and oral form, and to create, compile, or arrange, records and information with respect to the Government of Canada Public Key Infrastructure, whether or not derived from an investigation of the facilities of the Canadian Central Facility, collectively referred to as the ***Confidential Information***;

NOW THEREFORE, in consideration of the Government of Canada making the Confidential Information available to X, X agrees on its behalf, and agrees to cause its directors, officers, employees, agents and advisors:

(i) not to use for any purpose any portion of the Confidential Information, or notes, summaries or other material prepared by X or derived from any inspection conducted by Xor from X's evaluation of the Confidential Information (*referred to as X's "Notes")*, except to determine whether X wishes to issue a cross-certificate to the Canadian Central Facility;

(ii) not to disclose to others any portion of the Confidential Information or X's Notes, except to those employees, agents, advisors, consultants and other representatives of whom X has notified the Government of Canada in writing and who have agreed in writing to be bound by the terms of this agreement (*X's "Permitted Representatives")* and then only for the purpose described in clause (i) above;

(iii) not to make copies or otherwise reproduce the Confidential Information or any part thereof, or remove any of the Confidential Information from the place where it is made available, except:

[3] For use with private sector entities on government (TBS) letterhead.

(a) in the form of Notes made by X or X's Permitted Representatives during X's inspection of the Confidential Information to assist X in evaluating the proposed cross-certification; or

(b) as permitted with the specific written consent of the Government of Canada;

(iv) to maintain in a secure place X's Notes and copies of any part of the Confidential Information in the possession of X or X's Permitted Representatives and to take all steps reasonably necessary to ensure that no one other than X's Permitted Representatives will have access thereto; and

(v) not to assert or allege the existence of any representation, warranty or agreement by any of the Interested Parties, it being the intent of this clause that none of the Interested Parties shall have any liability or obligation to X except in respect of any representations, warranties and agreements which are in writing and hereafter duly executed by them. The Confidential Information is being given to X without liability on the part of the Government of Canada and no representation or warranty with respect to the Confidential Information is made by the Government of Canada or its employees, agents, contractors, representatives or advisors (*the "Interested Parties")*; and

(vi) if the Government of Canada withdraws its request for cross-certification, or if X decides not to issue a cross-certificate to the Canadian Central Facility, then X shall forthwith, without further notice, either:

(a) deliver to the Government of Canada, or as it may direct, the Confidential Information and X's Notes related thereto, without retaining any copies or extracts therefrom; or

(b) deliver to the Government of Canada, or as it may direct, a certificate that X has destroyed the Confidential Information and X's Notes related thereto, without retaining any copies or extracts therefrom.

X agrees to comply with clauses (i) through (v) for a period of five years.

If X is required at any time by law to disclose any portion of the Confidential Information or X's Notes, X shall provide the Government of Canada with prompt written notice of such requirement so that it may either seek an appropriate court order which would have the effect of relieving X of the requirement to disclose or else waive X's compliance with the provisions of this agreement. If the protective court order or other remedy is not obtained and the Government of Canada does not waive compliance, X agrees to furnish only that portion of the Confidential Information or X's Notes which X is advised by legal counsel is legally required and to use X's best efforts to ensure that confidential treatment will be accorded to that portion of the Confidential Information or X's Notes. X will not have any liability to the Government of Canada for disclosing Confidential Information or X's Notes in accordance with this paragraph.

Notwithstanding the foregoing, Confidential Information is not subject to the terms of this agreement if it consists of:

(i) documents already in X's possession before being disclosed to X under this agreement, unless designated as confidential or otherwise protected on their face or in an attachment;

(ii) documents or information in the public domain at the time of disclosure to X or which, after disclosure to X, enter into the public domain through no fault of X's or of X's Permitted Representatives

X agrees that Interested Parties shall be entitled to equitable relief, including injunction and specific performance, in the event of any breach of the provisions of this agreement, in addition to all other remedies available to the Interested Parties at law or in equity and X agrees that an award of damages may not be an effective remedy to the Interested Parties in the event of a breach of this agreement. X agrees to indemnify and hold harmless the Interested Parties from any damages, loss, cost or liability (including legal fees and the cost of enforcing this indemnity) arising out of the breach of this agreement by X or any of X's Permitted Representatives.

It is understood and agreed that no failure or delay by the Interested Parties in exercising any right, power or privilege under this agreement will operate as waiver therefor, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege under this agreement.

If any provision of this agreement or any part thereof is held to be invalid or unenforceable in whole or in part, such invalidity or unenforceability shall attach only to that provision or part thereof and the remaining part of that provision and all other provisions hereof shall continue in full force and effect.

This agreement shall be governed by and construed in accordance with applicable laws in force in the Province of ....and the laws of Canada applicable thereto, exclusive of their conflict-of-laws principles.

Her Majesty the Queen in right of
Canada as represented by the President
of the Treasury Board of Canada

....

Date:...

Signed on behalf of X

....

Date:..

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 3 - REQUEST REVIEW REPORT

The purpose of this report is to detail the results of a preliminary review by the PMA Desk Officer of the Candidate CA's request for cross-certification with the GOC PKI. The Desk Officer will conduct a preliminary review to ensure the CCA meets the required criteria to cross-certify with the GOC PKI and has met the document requirements. A preliminary analysis will determine if there is any obvious policy, administrative, technical, legal and financial issues that would impede entering into the cross-certification process.

The document is to be organized in the following manner:

1. Executive Summary

Candidate CA
Sponsoring Department
Key issues and rationale
Recommendations

2. Description of CCA and sponsoring agency endorsement

3. Business Rationale for Considering this Request for Cross-Certification

4. Description of Issues, if any

Policy
Administrative
Technological
Legal
Financial

5. Analysis of possible implications associated with cross-certification

6. Key issues for consideration and rationale

7. Recommendations

Proceed
Proceed with conditions
Do not proceed

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 4 - CROSS-CERTIFICATION TEAM – TERMS OF REFERENCE

A GOC PKI Cross-certification Team will have responsibility for the review and recommendation for acceptance/non-acceptance of specific cross-certification requests between an internal/external PKIs and the GOC PKI. This team, under the guidance of the Policy Management Authority (PMA), will interact with the Candidate CA to review and make recommendations with respect to cross-certification with the Candidate Ca with the Canadian Central Facility.

The mandate of a GOC PKI Cross-certification Team is to conduct all activities in Phases II and III that are assigned to it as per the GOC PKI Cross-Certification Methodology and report its findings to the PMA.

Tasks

The GOC PKI Cross-certification Team is responsible for ensuring that the following tasks are done:

1) review of Certificate Policy (CP) Mapping Standards;
2) review of GOC PKI CP;
3) examination of Candidate CA CPs;
4) examination of Candidate CA Certification Practice Statement (CPS);
5) review of PMA directions;
6) CP Mapping Report;
7) Testbed Trial Report;
8) ITS and Policy Compliance Certificate;
9) ITS and Policy Compliance Evaluation Report;
10) System Survey;
11) legal arrangements for cross-certification;
12) Negotiation Report;
13) Consolidated Evaluation Report, and
14) such other tasks as assigned by the PMA

Membership and Expertise

The GOC PKI Cross-certification Team comprises personnel with a range of professional backgrounds: technical, policy, legal and administrative. Collectively, the GOC PKI Cross-certification Team has a comprehensive understanding of the GOC PKI and all relevant issues.

A GOC PKI Cross-certification Team Leader will be designated from the team members. The Team Leader will interact and liaise on an “as-required” basis with the appropriate personnel (e.g. the POC of the Candidate CA, the sponsor).

The GOC PKI Cross-certification Team Leader will be the representative to the GOC PKI Secretariat and, as required, the PMA.

The GOC PKI Cross-certification Team requires personnel with expertise in the following areas:

1) legal issues;
2) CPs and CPSs;
3) GOC PKI technology;

4) Compliance Inspections;
5) IT security and technology and
6) Other areas as required (e.g., international relations).

ANNEX 5 – CP MAPPING SHEETS

Name of Organization: Date:

Negotiation Team Member: Registration Number:

Type of Document Information (circle one)

1. Digital Signature CP; Encryption CP; Combined CP/CPS

2. OID:

3: URL:

4. Level of Assurance(s): Rudimentary: Basic; Medium; High

Compliance Inspection Document Information

5. Compliance Inspection: Y N

6. Internal of External

7. Date Completed (yyyy/mm/dd):

8. Inspection performed by (name of firm, individual):

9. Level of assurance approved: Rudimentary; Basic; Medium; High

10. Comments:

CATEGORY/ELEMENT	**M/D**	**GoC PKI CP SECTIONS**	**Comparable Section**	**Comments**	**C**
Community and applicability	D	1.3			
Community of interest	D	1.3.1-1.3.5			
Applicability and intended applications	D	1.3.6, 1.3.6.1			
General provisions	M	(2)			
Liability	M	2.2, 2.2.4			
Obligations	M	2.1, 2.1.1, 2.1.1.2, 2.1.1.4, 2.1.2			
Financial responsibilities	M	2.3			
Compliance with laws and regulations	M	2.4			
Identification and Authentication	M	3, 5.2.3			
Initial registration	M	3.1.1, 3.1.2			
Authentication of Entities	M	3.1.8, 3.1.9, 3.1.10, 3.2, 3.3, 3.4			

CATEGORY/ELEMENT	**M/D**	**GoC PKI CP SECTIONS**	**Comparable Section**	**Comments**	**C**
Operations policy	M	4			
Certificate application	M	4.1			
Acceptance	M	4.3			
Revocation	M	4.4, 4.8.2			
Suspension.	D	4.4			
Key compromise	M	4.4.1, 4.8.3, 4.4.15, 2.1.3.4			
Audit policy	M	4.5			
Records and records keeping	M	4.6			
Compliance audit	M	2.7			
Confidentiality	M	2.8			
Business resumption	M	4.8			
Termination	M	4.9			
Local security policy	M	5, 6			
Physical controls	M	5.1			
Procedural controls	M	5.2			
Personnel controls	M	5.2.3, 5.3			
Technical controls	M	6, 6.1			
Security controls	M	6.2, 6.5, 6.6, 6.7, 6.8			
Key management policy	M	6, 6.2, 6.3, 6.4			
Key Protection;	M	2.1.1.5, 2.1.2.3, 2.1.3.2, 6.2			
Key Delivery;	M	6.1.2, 6.1.3, 6.1.4			
Key Escrow;	M	6.2.3			
Key Backup;	M	6.2.4			
Key Archive;	M	6.2.5, 6.3.1			
Key Expiration	M	6.2.9			
Key Usage	M	6.1.9, 6.2.2			
Validity period of public and private keys	M	6.3.2			
Certificate and CRL Profile	M	7			
Certificate version	M	7.1			
CRL version	M	7.2			
Policy administration	D	8			
Policy authority and contact details	M	1.4			
Publications and Repository	M	2.6			

Notes:

1. M = Mandatory – category or element must be present
2. D = Desirable – category should be present
3. C = special considerations, Cross-Certification Team should use [C= critical (possible failing condition); F = flag (further examination required, i.e. details in CPS); W = warning (small difference not critical); no mark section ok

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 6 - CP MAPPING REPORT

The purpose of this report is to detail the results of the policy mapping process comparing the CCAs CPs with the GOC PKI CPs. The Cross-Certification Team will perform the policy mapping using the CP Mapping sheets.

The document is to be organized in the following manner:

1. Executive Summary

CPs mapped to GOC PKI CP
Any discrepancies
Key issues and rationale
Recommendations

2. Description of CPs mapped to GOC PKI CP

3. Description of Issues, if any

Discrepancies
CP references

4. Analysis of possible implications

5. Key issues for consideration and rationale

6. Recommendations

Proceed
Proceed with conditions
Do not proceed

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

SYSTEM SURVEY QUESTIONNAIRE

CROSS-CERTIFICATION WITH THE GOVERNMENT OF CANADA PUBLIC KEY INFRASTRUCTURE (GOC PKI)

V 1.0

ANNEX 7 - SYSTEM SURVEY QUESTIONNAIRE

Purpose:

The purpose of the System Survey Questionnaire (SSQ) is to evaluate the technical functionality requirement of the candidate CA to ensure compatibility and interoperability with GOC PKI.

Methodology:

The System Survey questionnaire has been categorized in 3 groupings: Administrative, Maintenance and Support, and Network Architecture. The SSQ is to confirm the system readiness and is being distributed to the candidate CA requesting to cross-certify with the GOC PKI Canadian Central Facility (CCF).

Reference documents:

a. Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999
b. Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, March 1999
c. Internet X.509 Certificate Request Message Format, RFC 2511, March 1999
d. PKCS #10: Certification Request Syntax Version 1.5, RFC 2314, March 1998
e. ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997
f. Recommendation X.509 and ISO 9594-8, Information Processing System - Open Systems Interconnection - The Directory - Authentication Framework, 1988.
g. ITU-T Recommendation X.830 (1994) | ISO/IEC 11586-1:1996, Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Overview, Models and Notation
h. ITU-T Recommendation X.831 (1994) | ISO/IEC 11586-2:1996, Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element (SESE) Service Definition
i. ITU-T Recommendation X.832 (1994) | ISO/IEC 11586-3:1996, Information Technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element (SESE) Protocol Specification

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
1.	***Administration***		
1.1	**Point of contact (POC):** • name(s) • address • phone, fax, email numbers		
1.2	**Specific location of facility:** • building address • floor • room		
1.3	**System access:** • visit clearances (or security clearance) • general process: ▪ visit notice required ▪ sign-in ▪ escorts		
2.	***Maintenance and Support***		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
2.1	**System prime representatives for the purpose of problem reporting and information exchange amongst system primes.** • name(s) • position • address • phone, fax, email numbers		
3.	***Network Architecture***		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.1	**Environment:** Can you provide a high level overview of the candidate CA system and network architecture for the following environment? • development (Test lab) • production • other (Disaster Recovery Site) Please include a general description of the candidate CA's: • Firewall, • Router, • Key Management/Server, • X.500 Directory, • Administrator Workstations, and • connectivity to the Internet.		
3.3	**Firewall Software** Please identify the firewall application software (by release number, including all incorporated patches, if any) used by the candidate CA.		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.4	**Firewall Access Policy** Please provide a summary of the candidate CA's firewall access policy. For example, the policy is expected to address issues such as: • Identification of proxies by type and associated privileges – e.g. FTP sessions, TCP proxy, LDAP proxy, DSP bindings, etc. • Traffic source and destination including port numbers		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.5	**Firewall Functional Requirements :** Is your firewall capable of being configured to address each of the following functional requirements? Please identify those (if any) that your firewall is incapable of supporting? Are there any additional capabilities of your firewall that are not addressed by the following? Please identify. The firewall is expected to have no fewer than the following capabilities: • Packet filtering in a proxy mode whereby all packets are checked for: ▪ Source and destination IP address ▪ Protocol type ▪ Protocol command type ▪ Bi-directional checking of TCP sequence and port numbers • Support port and/or IP address filtering/blocking • Block source routed IP packets • Support packet routing • Support independent inbound/outbound access control policies		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.4	**Firewall Audit Events:** Please describe the candidate CA firewall generated audit event capabilities. For example, such a firewall is expected to generate an audit event for no fewer than the following items per each attempted session: • Session outcome (success or failure) • Source/destination IP address(es) • Protocol type • Source/destination port number(s) • Proxy used • Session duration • Number of bytes transmitted • Date and time		
3.5	**Firewall Audit Event Grouping:** Please describe the audit trail capabilities provided by the candidate CA firewall. For example, it is expected that the firewall should be able to group audit events in no fewer than the following categories: • Events associated with connection requests • Events associated with data exchanges between networks • Events associated with CA enabled services		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.6	**Firewall – Trusted Time Source:** Does the candidate CA utilize an external source of trusted time? If so, what port number is used?		
3.7	**Router:** Please identify the router used by the candidate CA. In so doing, please: • State the router model • State the software version release used by the router • State whether or not the router supports dial-up links • Describe how the operator manages the router configuration.		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.8	**<u>Router Functional Capabilities:</u>** **Specifically address whether your Router addresses each of the following (suggested) functional requirements:** • Provides a number (please state) of 10Base-T interfaces, each of which support line speeds up to no less than 10 Mbps • Supports the full suite of the TCP/IP protocol family • Supports high speed synchronous or ISDN WAN interfaces using line speeds in the range from 19.2 Kbps to T1 • Supports at least one of: ▪ Frame relay, ▪ T1 framing, or ▪ ISDN WAN links • Supports OSPF and RIP routing protocols. • It is also desirable that it support the IGRP/EIGRP protocol. • Provides a number (please state) of 10Base-T Ethernet LAN interfaces. • It is desirable that the router support both Thinnet (coax cable) and Thicknet (AUI) • Supports filtering by: ▪ Protocol, ▪ IP address and ▪ TCP port.		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.9	**Ethernet Hub Description:** **Please provide a description of the Ethernet Hub used by the candidate CA. For example, the GOC PKI Ethernet Hubs all have the following functional capabilities:** • Utilize 10Base-T interfaces, each of which support line speeds up to no less than10 Mbps • Upgradeable to 100Base-T interface hardware should it be warranted • Separate 10Base-T hubs are used to segregate the Ethernet segments ensuring traffic separation and security • Each 10Base-T hub supports a minimum of four (4) 10Base-T Ethernet LAN physical interfaces • Supports both Thinnet (coax cable) and Thicknet (AUI) • The Ethernet hub is expandable to 24 ports		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.10	**Key Management Application:** • What PKI Key Management application software (e.g., Entrust/PKI Version 5.0) does your CA use? Please specify the software release of the Key Management software. • What is the IP Address of the server which hosts the PKI key management software? • What is the port number used for cross-certification? • What is the CA Distinguished Name?		
3.11	**X.500 Directory:** • What X.500 application software and release number is your CA using? • Upon which operating system is the X.500 directory hosted? Please specify the release version in use.		
3.12	**X.500 Directory:** Is your X.500 Directory compatible with commercial X.500 Directories that comply with the Lightweight Directory Access Protocol (LDAP) interface requirements?		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.13	**X.500 Directory:** What version of LDAP does your directory support? Note: • LDAP v2 is defined by RFCs 1777 – 1779, 1959 and 1960 • LDAP v3 is defined by RFCs 2251 – 2256 inclusive		
3.14	**X.500 Directory:** What standards are being followed for your X.500 Directory? • PKIX. • IETF. ● Others (Specify)		
3.15	**X.500 Directory:** Is your X.500 Directory available to the public in general?		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.16	**X.500 Directory:** What is your internal X.500 Directory Information Tree (DIT) structure? • Host naming convention • User naming convention • Group naming convention • X.500 Naming convention for nodes and leaf entries (e.g. cn + serialNumber)		
3.17	**X.500 Directory Chaining:** Please provide the following information in order to ensure that the CCF and candidate CA can chain their directories: • the Common Name of the DSA • the IP address of the DSA • the TCP port number used for chaining • the Transport Selector for the DSA		
3.18	**Candidate CA Distinguished Name:** What is the DN of the candidate CA? For example, the GOC PKI CA DN is: c=CA, o=GC, ou=CCF-ICC, ou=1CA-AC1		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.19	**X.500 Directory:** What is your X.500 DSA requirement? The GOC PKI is compliant with: • X.509 version 3 certificates in accordance with PKIX • X.509 version 2 CRL in accordance with PKIX		
3.20	**X.500 Directory:** Can your DSA support anonymous chaining requests?		
3.21	**X.509 Certificate Format:** Does the candidate CA generate base certificates that comply with Recommendation X.509 IS0/IEC 9594-8: 1993?		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.22	**X.509 Certificate and CRL Extensions:** Please describe the Certificate and CRL Extensions supported by the candidate CA specifically addressing the following: • Key (i.e. authorityKeyIdentifier, subjectKeyIdentifier, keyUsage) and Policy (i.e. certificatePolicies) Information (specifically addressing the **policyMappings** extension used specifically for cross-certification); and • CRL Identification (i.e. authorityKeyIdentifier)		
3.23	**X.509 PKIX CMP Compliance:** Please state the degree to which the candidate CA PKI Key Management application identified earlier at 3.10 supports key transfer pursuant to the Internet X.509 Public Key Infrastructure Certificate Management Protocol defined by RFC 2510 dated March 1999.		
3.24	**Certification Request Syntax:** In conjunction with 3.24, please confirm that the candidate CA PKI Key Management application identified earlier at 3.10 supports PKCS #10: Certification Request Syntax Version 1.5 (RFC 2314 dated March 1998).		

Table 1 - Cross Certification System Survey Questionnaire

#	INFORMATION REQUIRED	DESCRIPTION	REMARK
3.25	**Secure Exchange Protocol Compliance:** In the event that the candidate CA PKI Key Management application identified earlier at 3.10 does not support PKIX-CMP (refer to 3.23), please state the degree to which the application supports key transfer using a secure exchange protocol based upon a sub-set of the Generic Upper Layers Security (GULS) standard defined by the following: • X.830 (1994) | ISO/IEC 11586-1:1996 • X.832 (1994) | ISO/IEC 11586-2:1996 • X.833 (1994) | ISO/IEC 11586-3:1996		
3.26	**PKIX Certificate and CRL Extensions:** Please describe the certificate and CRL extension PKIX profile of the candidate CA. In the event that the candidate CA is not using Entrust Version 5.0 or equivalent, the candidate CA will need to comply with the minimum PKIX profile, as defined in e. ITU-T Recommendation X.509, and identified in Table 2 (refer to page 59)		

Table 2 - CA Minimum PKIX Compliance

Element	CA Support
Certificate extensions	
authorityKeyIdentifier	Yes
subjectKeyIdentifier	Yes
keyUsage	Yes
certificatePolicies	Yes
subjectAltName	Yes
basicConstraints	Yes
nameConstraints	Optional
policyConstraints	Optional
extKeyUsage	Optional
cRLDistributionPoints	Optional
CRL extensions	
authorityKeyIdentifier	Yes
CRLNumber	Yes
CRL entry extensions	
reasonCode	Optional
invalidityDate	Optional

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 8 - TESTBED TRIAL REPORT

The purpose of this report is to document the Testbed Trial results to determine if there has been a successful exchange of certificates between the CCA and the CCF and if the certificates can be validated. The Cross-Certification Team will collaborate with the CCF in producing this report.

The document is to be organized in the following manner.

1. Executive Summary

Testing results
Any discrepancies
Key issues and rationale
Recommendations

2. Description of Testbed Trial activities and methodology

Testing results
Description of discrepancies

3. Analysis of discrepancies and implications associated with cross certification

4. Key issue for consideration and rationale

5. Recommendations

Proceed
Proceed with conditions
Do not proceed

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 9 - INFORMATION TECHNOLOGY SECURITY CHECKLIST

Institution Name:	Address:
Reference Number:	
Inspection participant(s):	Date:
Negotiation Team Member(s):	Date of any previous Inspections:
Level of Assurance:	Internal or external to the GOC PKI:
□ Medium-Level Assurance	□ Internal □ External

ADMINISTRATIVE AND ORGANIZATIONAL

Appointment of Security Personnel

Item	Activities	Yes	No	Comments
1	Has an IT security representative been appointed for the CA physical domains?			
2	Have CA employees been assigned responsibility for the CA security aspects of personnel, physical and environment, hardware, software, operations, and communications?			

Security Policy

Item	Activities	Yes	No	Comments
3	Do you have a set of CA IT security policies?			
4	Does your CA password policy for the CA systems include the following: • At least 8 characters in length? • Not to be recorded or divulged? • Changed at least every 3 months? • Excluded from scripts?			

Security Procedures

Item	Activities	Yes	No	Comments
5	Do you have a set of CA IT security procedures?			
6	Do you have a procedure for security incident handling?			

Item	Activities	Yes	No	Comments
7	Do you have a procedure for monitoring activities during periods of privileged access?			
8	Do you have a procedure for de-briefing, revoking of access privileges, and returning security-related items when employment of CA personnel and/or contractor are transferred or terminated?			
9	Do you have a procedure for the maintenance of CA hardware, software, communications, network and environmental components, and IT media?			
10	Do you have a problem management procedure for all CA system components?			
11	Do you have a procedure to define priorities and conditions for escalation?			
12	Do you have a change management procedure for all CA system components?			
13	Do you have a procedure for the handling, transport, transmittal, sanitation, and destruction of particularly sensitive (Protected "B") CA IT assets information for the following: • Transport and transmittal of CA back-up cartridges to and from the cold back-up site? • Transfer of CA hardware components to an external organization for service and maintenance? • Distribution of CA subscriber initialization data (reference numbers and authorization codes)?			
14	Do you have a procedure to verify hardware/software security configuration and mechanisms for the following: • Attempt to log on with invalid user ID? • Attempt to access files for which CA personnel have not been granted privileges? • Attempt to use privileged software?			

Item	Activities	Yes	No	Comments
15	Does your procedure to obtain root password and use root on the CA systems include the following: • Root account on all CA systems being used for emergency purposes only? • CA employees requiring root privileges must be given a personalized account? • Root passwords must be kept in a sealed, dated, and signed envelope which is to be stored in an approved container within the CA? • Access to root passwords must be approved by the CA Manager and the use of the root account monitored?			
16	Do you have a procedure for testing hardware, software, communications and network components prior to implementing in the production environment, and migration to the production environment?			
17	Do you have a procedure to verify on a weekly basis the integrity and consistency of the CA database and the X.500 Directory?			
18	Do you have backup and compare procedures according to the following schedule: • Daily backups, retention period of 7 days – ➢ Full backup of the CA database? ➢ Full backup of the CA X.500 Directory? • Weekly backups, retention period of 1 month – ➢ Full image backup of CA Manager system's hard drive? • Monthly backups, retention period of 1 year – ➢ Full image backup of CA Manager system's hard drive?			

Item	Activities	Yes	No	Comments
19	Do you have operation procedures for the following: • Power up/power down sequence for all CA systems? • Start up/shut down of CA systems? • Hardware component operation? • Start and stop CA communications? • Emergency situations? • Procedures for update of certification revocation list (CRL)? • Procedure for recovery of CA subscriber encryption key pair? • Procedures for CA systems maintenance?			
20	Have procedures been developed and implemented to allow removable IT media containing CA information to be placed in a protected status and used only with written authorization?			
21	Have procedures been developed and implemented for the handling, protection, and accountability for all removable IT media entering, remaining within, and leaving the CA environment?			
22	Have verification procedures for CA backups been developed and implemented to ensure backups were successful?			
23	Have procedures been developed and implemented for the preparation, issuance, change, cancellation and audit of CA personnel identifiers?			
24	Have procedures been developed, documented, and implemented for reporting, recording, tracking, and resolving CA hardware, software, communications, network and environmental components, and IT media problems affecting security?			
25	Do you have a procedure to conduct and document security review of the CA IT-related activities that includes the following items and frequencies: • Review TRA – annually? • Review CA IT security – annually? • Review and test CA contingency plan – annually?			

Item	Activities	Yes	No	Comments
	• Review CA Environmental component maintenance log – annually? • Review CA hardware configuration chart, inventory, and minimum requirements – ➢ Annually? ➢ When planning changes? • Review configuration of CA hardware/software protective mechanisms and run tests – ➢ Monthly? ➢ When planning changes? • Audit of CA communications – annually? • Review CA contracts – annually? • Review CA communications configuration chart, inventory, and minimum requirements – annually? • Review CA software configuration and inventory – annually? • Review CERT, BugTraq and CIAC advisories – weekly?			

Statements of Sensitivity (SOS)

Item	Activities	Yes	No	Comments
26	Has a CA statement of sensitivity specifying the security designation, availability requirements, and integrity concerns of the CA systems been prepared?			
27	Is the CA statement of sensitivity available to personnel responsible for the security of the CA systems?			

Contracting

Item	Activities	Yes	No	Comments
28	Do contracts include a configuration chart agreed upon by the CA Manager and the contractor?			
29	Have configuration changes made during the period of the contract been documented, reported, reviewed, and approved prior to implementation?			
30	Did configuration changes made during the period of the contract reduce the level of security provided?			
31	Has the CA specified security requirements in all contracts with external organizations where those contracts affect the CA services, information, or system components for the following:			

Item	Activities	Yes	No	Comments
	• Hardware components? • Software components? • Communications components? • Network components? • Any related services controlled by contractor?			

Threat and Risk Assessment (TRA)

Item	Activities	Yes	No	Comments
32	Has a CA TRA been prepared and maintained, outlining existing and proposed safeguards and describing threats and risks of which account has been taken on the following: • System interconnections? • Communications components? • Network components?			

Access Control and Authorization

Item	Activities	Yes	No	Comments
33	Have access privileges to the CA been authorized and controlled for: • Users? • Operations personnel? • Maintenance and support personnel? • Systems analysis and programming personnel?			

Security Logs and Records

Item	Activities	Yes	No	Comments
34	Did the CA identify and document: • The types of CA security activities and events to be monitored? • The method of determining how activities and events are to be monitored? • The type of records to be kept? • How and when the security information is to be reported?			
35	Are the CA security logs, documents, and records being retained for one year?			

Change Control

Item	Activities	Yes	No	Comments
38	Are all changes to CA hardware components being centrally controlled and documented?			

Problem Reporting

Item	Activities	Yes	No	Comments
39	Are CA systems problems affecting security being immediately reported to the Departmental and/or Organizational IT security coordinator?			
40	Is a contact list identifying CA systems support personnel, field service personnel, communications software services personnel, data communications vendors, and telecommunications carriers being maintained?			

Contingency Planning

Item	Activities	Yes	No	Comments
41	Did the CA define and document the essential levels of service and the maximum acceptable periods of downtime for the CA systems?			
42	Does your contingency plan been developed, documented, and maintained to ensure the essential level of CA service (on-site and off-site) will be provided following any loss of processing capability or destruction of a CA facility include the following: • Recovery of master keys and CA key pairs? • Recovery of any failure of CA system components? • Recovery of the CA facilities and any wiring closet from fire? • Re-establishment of CA services following destruction of the secure room(s) or the building/complex? • Recovery from a redundant unit failure? • Forced evacuation of a CA physical domain or the building/complex? • Strikes? • Bankruptcy of critical suppliers? • Loss of critical environmental components? • Security requirements during contingencies? • Identification of essential systems, information resources, personnel (including support), and phone numbers? • Recovery of the CA database and the X.500 Directory following hardware crashes?			

Item	Activities	Yes	No	Comments
43	Does your cold back-up site have physical and environmental safeguards?			
44	Is your cold backup site location subject to the same physical and environmental threats as your primary site?			
45	If the CA contingency plan requires the use of facilities not under the control of the CA, have formal agreements or contracts for the use of such facilities been established and reviewed annually?			
46	Does the CA ensure that the implementation of the CA contingency plan does not compromise confidentiality or integrity requirements?			
47	Is the CA contingency plan being tested annually to the extend practicable and does it remain consistent with security?			
48	Are there sufficient alternate trained personnel to assure the confidentiality, integrity, and availability of the CA?			
49	Have employees identified to take an active role in CA-related contingency situations received training and practice in their assigned duties?			
50	Are the following items being stored off-site: • CA contingency plan, procedures, and agreements? • Hardware configuration chart, hardware component inventory, and minimum hardware configuration requirements? • Communications configuration chart, communications hardware component inventory, and minimum communications configuration requirements? • Operating Systems software, utilities, and documentation? • Applicable product (e.g. Entrust and X.500) application software and documentation? • Current copy of the CA database and the X.500 Directory? • At least one CA Master User’s password, one CA security officer’s password and one CA administrator’s password in a sealed, signed, and security marked envelope? • Root account passwords in a sealed, signed, and security marked envelope?			

Item	Activities	Yes	No	Comments
	• CA forms? • Cold back-up site log of CA back-up cartridges stored at that location?			

PERSONNEL

Security Screening

Item	Activities	Yes	No	Comments
51	Has the CA Manager been assigned the following responsibilities: • Verify that the appropriate security screening type and level has been specified for each position and contract? • Ensure that CA personnel and contractors have been security screened at the level specified for their position or contract prior to authorizing access to CA systems and resources?			

Security Awareness

Item	Activities	Yes	No	Comments
52	Have security briefings been given to personnel and contractors who have access to the CA include the following: • Access requirement of their position? • Authorized security screening level? • Responsibilities for safeguarding CA assets? • Departmental/Organizational IT security rules and regulations?			
53	Are the security briefings conducted in person, where possible?			
54	Does the security briefing include the following: • A written document outlining the contents of the briefing and date given? • A signed document by the person being briefed indicating the receipt of, and agreement to, its contents?			

Training of Personnel

Item	Activities	Yes	No	Comments
55	Do you have a CA training program and material which includes as a minimum:			

Item	Activities	Yes	No	Comments
	- IT security principles? - CA security features and vulnerabilities? - CA and applicable products (e.g. Entrust and X.500) application software training to all CA personnel? - Privileged access to CA systems? - CA contingency plan? - Operating Systems training for CA Master Users? CA security officers, CA administrators, and CA support specialists?			

PHYSICAL AND ENVIRONMENTAL

Facility

Item	Activities	Yes	No	Comments
56	Do physical and environmental security safeguards for the CA facilities (wiring closet and secure rooms) in accordance with the Departmental and/or Organizational standard for IT facilities include the following: - Restricted zone sign? - Slab-to-slab walls? - Approved dead bolt and cipher lock? - Access limited to authorized personnel? - Visitors authorized and escorted? - Access from a Security zone? - Monitored 24/7 by a combination of CA personnel and electronic intrusion detection systems?			

Restricted Zones

Item	Activities	Yes	No	Comments
57	Is access to the CA physical domains controlled, authorized and monitored as appropriate to IT facilities for the following: - Entry points? - Personal recognition? - Personal identification? - Electronic access control? - Electronic intrusion detection (EID)? Closed-circuit television (CCTV)?			

Item	Activities	Yes	No	Comments
58	When servicing CA system components, are maintenance and service personnel properly escorted and supervised by knowledgeable and authorized CA personnel?			

Security Containers

Item	Activities	Yes	No	Comments
59	Do IT media containing sensitive CA assets (including magnetic cartridges, diskettes, removable hard drives, and computer printouts) meet the following criteria: • Stored in approved Protected "B" containers and locks? • Located in an appropriate restricted zone?			
60	Are keys and combinations for containers storing sensitive CA assets issued only to authorized personnel and properly controlled?			

Methods of Controlling Access

Item	Activities	Yes	No	Comments
61	Are the identities and the authorization of individuals being authenticated verified prior to granting access to CA facilities?			
62	Do appropriate methods implemented to control access to CA facilities include the following: • Installing electronic access controls, mechanical combination locksets, or deadbolts? • Limiting the number of entry points to the minimum required by fire regulations?			

Method of Authorizing Access

Item	Activities	Yes	No	Comments
63	Is an access list being maintained of persons authorized to access the CA physical domains?			
64	Do access records being maintained on non-CA personnel accessing CA physical domains include the following: • Name of person? • Person's employer or affiliation? • Name of the escort? • Restricted zone entered? • Date and time of entry?			

Item	Activities	Yes	No	Comments
	• Date and time of departure?			

Method of Monitoring Access

Item	Activities	Yes	No	Comments
65	Are records being maintained documenting issuance and retrieval of CA security-related items for the following: • Keys? • Door access codes? • Padlock combinations?			

IT Utilities and Services

Item	Activities	Yes	No	Comments
66	Are maintenance procedures consistent with the manufacturers' specifications being documented and implemented for the following environmental components: • Electrical systems? • HVAC systems? • UPS systems? • Fire protection systems?			
67	Are records maintained of all environmental component maintenance activities being: • Retained for a minimum of one year? • Reviewed annually?			
68	Are all environmental component faults being: • Recorded? • Brought to the attention of the CA Manager? • Actioned (Corrective action taken)? • Finalized (Final resolution recorded)?			

Electric Systems

Item	Activities	Yes	No	Comments
69	Do you have a UPS with power conditioning for the following hardware components: • CA systems and redundant units (excluding the workstation); • All firewalls, hubs, ROUTERS and communications equipment; and • Paging modems.			

Item	Activities	Yes	No	Comments
70	Are power services for CA hardware components equipped with power conditioners capable of providing a stable power supply?			
71	Have CA systems been configured so as to shutdown automatically (e.g. 10 minutes) prior to the maximum duration time of the UPS batteries?			

Destruction of IT Media

Item	Activities	Yes	No	Comments
72	Is IT media containing sensitive CA information being destroyed in an approved manner?			
73	While awaiting destruction or in transit to destruction, is IT media containing sensitive CA information being safeguarded according to the highest sensitivity of information?			
74	Is destruction of IT media containing sensitive CA information being monitored by an employee with a security screening level at least equal to the highest sensitivity of information?			

Disposal/Re-use

Item	Activities	Yes	No	Comments
75	Are erasable IT media previously used to store CA information being kept in the CA environment until the IT media has been sanitized using an approved erasure technique?			
76	Are erasable IT media and their containers being divested of all markings only after verification of the sanitation procedure?			
77	Are erasable IT media sanitized using an approved technique when CA hardware components are to be removed from the CA environment for servicing?			

IT Media - General

Item	Activities	Yes	No	Comments
78	Have write-protection mechanisms been enabled for all removable IT media containing CA information?			

IT Media Library

Item	Activities	Yes	No	Comments
79	Do records being generated for accountability of IT media include the following:			

Item	Activities	Yes	No	Comments
	• IT media identifier? • Identification of owner? • Date and time of transaction? • Details of transaction including appropriate authorization?			
80	Are controls for CA removable IT media stored in off-site locations commensurate with the designation of particularly sensitive (Protected “B”)?			

Markings

Item	Activities	Yes	No	Comments
81	Is IT media containing CA information assigned a security designation of particularly sensitive (Protected “B”)?			
82	Have security designations been clearly marked on all CA IT media on the casing and the outer container in plain language and eye-readable form?			
83	Have records concerning system authentication mechanisms, codes, or passwords used to authenticate identities been provided the designation of particularly sensitive and marked as Protected “B”?			
84	Are the following items considered particularly sensitive been marked as Protected “B”: • TRA? • CA IT security monitoring document? • Configuration charts, parameters, and inventories? • All CA lists and logs? • Forms containing CA subscriber initialization data? • CA back-up cartridges and other IT media containing CA data?			
85	Has ownership of all CA removable IT media been clearly indicated in eye-readable form on the IT media itself and on the containers used for such IT media when they are to be removed from the CA environment?			

HARDWARE

Configuration /Inventory

Item	Activities	Yes	No	Comments
86	Is the chart of the current CA hardware configuration, identifying all hardware components and interconnections (e.g. CPU, peripheral devices, channels, controllers, etc.) being maintained and reviewed at least annually or when changes are made?			
87	Does the current CA hardware inventory being maintained identify the following: • Manufacturer/supplier? • Model number? • Serial number? • Revision levels? • Micro-code levels? • Ownership?			

Security Prevention

Item	Activities	Yes	No	Comments
88	Is remote diagnostic access to CA system components being controlled at all times?			
89	Do all essential CA hardware components left powered up and unattended have an automatic power-down capability, which will respond to environmental conditions outside the specifications detailed by the supplier?			
90	Are the CA system components' protective mechanisms being checked periodically to ensure they are functioning properly?			
91	Have the CA and X.500 hosts been restricted to provide only CA and X.500 services and no additional non-PKI applications?			
92	Have all unnecessary services, including network services, been disabled on the CA and X.500 hosts, routers and firewall?			
93	Have the CA and X.500 hosts, routers and firewall operating systems been updated with the latest pertinent patches?			
94	Have all CA and X.500 host, router and firewall default names, especially administrator and root accounts, been appropriately renamed?			

Item	Activities	Yes	No	Comments
95	Have all user, group and system accounts, not explicitly required for provision and support of the CA and X.500 hosts and firewall and associated services, been removed or disabled?			
96	Have CA and X.500 hosts and firewall been appropriately configured to lock console or login sessions after a specified period of inactivity?			
97	Have appropriate security policies and restrictions been applied to user accounts (ie. password length, password age, password re-use, and account lockout)?			
98	Have appropriate permissions been assigned to CA and X.500 hosts files and directories to prevent unauthorized access and remove excessive user rights?			
99	Have all unnecessary network protocols been disabled on the CA and X.500 hosts?			
100	Have all TCP/IP ports been disabled on the CA and X.500 hosts except for those explicitly required to support the CA and X.500 services?			
101	Have all shared network resources that are not required for the support of the CA and X.500 services been disabled?			
102	Have all network services not explicitly required been disabled?			
103	Have all accounts not explicitly required been removed?			
104	Is the UNIX umask variable set so that new files and directories are automatically created with restrictive permissions?			
105	Are UNIX shell and CDE login sessions configured to be automatically locked or logged out after a specified period of inactivity?			

COMMUNICATIONS

Inventory

Item	Activities	Yes	No	Comments
106	Does the current CA communications components inventory being maintained and reviewed annually identify the following: • Whether an item is owned, rented or leased and the date of the last change?			

Item	Activities	Yes	No	Comments
	• Communication hardware and service, including – ➢ Circuits, lines or connections assigned, including the identification of the supplier? ➢ The location of the physical termination of the circuits and lines? ➢ IT media used (e.g. coaxial, fiber, unshielded twisted pair)? ➢ The circuit or line status assigned or available? ➢ The level of security classification or designation of each circuit or line? ➢ Hardware identifiers of remote input/output units? ➢ Communications hardware (document model number and serial number, e.g. modems, dial-ins, concentrators, packet switched devices, encryption devices, and data switches? • Communication software and data, including – ➢ Software programs? ➢ Configuration Database and files (libraries)? ➢ Software procedures (e.g. Command files)? ➢ Software utilities? ➢ Security-relevant components? ➢ License numbers? • Communications networks, including – ➢ Devices, e.g. servers, routers, gateways, bridges? ➢ Protocol and level? ➢ Network operating systems and applications software? ➢ Network IT media and transmission methods? ➢ Identification of node names (document: name, network address, type, location, responsible manager)? ➢ Security-relevant network applications, features and items?			

Item	Activities	Yes	No	Comments
107	Do CA inventory records for each communications software item include the following items: • Security designation? • Whether or not the item is considered privileged or powerful? • The quantity and their locations? • Identification of owner, custodian, authorized user and maintainer? • Date created or modified and version/level number?			
108	Do CA communications terminals and/or circuits identified by the following: • Labels affixed on or near the equipment? • Labels affixed on a diagram kept near the equipment? • Labels affixed to cables with unique identifiers?			
109	Have CA communications inventory items that are necessary for, or could affect the system's protective mechanisms been assigned and marked with the security designation of particularly sensitive (Protected "B")?			

Configuration

Item	Activities	Yes	No	Comments
110	Is a chart of the current CA communications configuration being maintained, reviewed annually, and marked with an issue date?			

Routine Maintenance

Item	Activities	Yes	No	Comments
111	Are the use of communications test equipment, privileged and powerful communications software utilities, network monitoring tools, and diagnostics for monitoring the network being authorized and controlled by the CA Manager?			

Operational and Control Procedures

Item	Activities	Yes	No	Comments
112	Are CA communications equipment being operated only by CA authorized personnel?			

Detection and Surveillance

Item	Activities	Yes	No	Comments
113	Are tests of security features being conducted periodically to ensure CA communications controls have not been compromised or misused?			
114	Are results of these security features tests recorded for audit and quality assurance purposes?			

Protection of Information in the CA Communications Environment

Item	Activities	Yes	No	Comments
115	Is direction and guidance for COMSEC being obtained from the Departmental COMSEC Authority?			
116	Does the Departmental COMSEC Authority select the approved encryption technique?			
117	Has a CA encryption key management plan been developed?			

SOFTWARE

Inventory

Item	Activities	Yes	No	Comments
118	Do CA software inventory records being maintained include the following: • System software? • Database software? • Application software? • Access control software? • Software utilities? • Software procedures and command files? • Program and procedure libraries and directories? • Database and data files? • Operational configuration parameters?			
119	Do CA software inventory records for each item indicate: • The security designation? • Whether the item is considered privileged or powerful software? • Warranty/maintenance conditions? • The number of copies or valid users along with their physical locations? • The owner, custodian, authorized user,			

Item	Activities	Yes	No	Comments
	and maintainer? • A creation/modification date, version/level number, and any special modifications?			

Surveillance

Item	Activities	Yes	No	Comments
120	Are CA surveillance and protective mechanisms being tested at least annually, or following changes to security-relevant software, to ensure continued capability of the system to prevent: • Access to CA systems and data resources? • Access to residual data? • Use of privileged capabilities? • Read or write from outside allocated memory bounds?			
121	Do CA systems recording security-relevant events include the following: • File, volume, and database accesses? • Communications device connect, disconnect, and re-configuration? • Network status messages? • User sign-on and sign-off? • System operator commands and responses? • System-generated messages or requests regarding configuration changes? • Changes to system logging facility status? • Changes to access control information? • Changes to lists of authorized users? • Detected security incidents? • Use of privileged or powerful software?			
122	Has the following information, if applicable, been recorded for each security event: • Nature and type of incident? • Date and time? • User identification? • Device identification? • Job or process identification? • Identification of resource accessed? • Mode of access? • Configuration details?			

Data and Database Administration

Item	Activities	Yes	No	Comments
123	Have audit checks of the CA database and the X.500 Directory been conducted to verify the logical and physical consistency of the database and identify discrepancies such as lost records, open chains, and incomplete sets?			
124	Have CA database maintenance utilities that bypass controls been considered to be privileged and powerful software that must be restricted and monitored?			

OPERATIONS

Operating Procedures

Item	Activities	Yes	No	Comments
125	Are hardware and software techniques in place to detect hardware/software/communications/ network failures in the following: • Primary CA systems? • Back-up CA systems? • Standby CA systems?			
126	Are sufficient generations of CA backup data being maintained to ensure that data can be recovered?			
127	Is the two person integrity principle applied to the following functions: • Setting certificate lifetimes? • Cross-certification operations? • Creation of CA Master Users, CA security officers and CA administrators? • CA systems master key updates? • Adding and deleting CA security officers? • CA security officer password changes?			
128	Is remote access to CA system components for diagnostic purposes prohibited?			
129	Are the CA operating systems and product (e.g. Entrust) application components designated as particularly sensitive information being safeguarded accordingly?			

Item	Activities	Yes	No	Comments
130	Is the use of privileged and powerful software prohibited unless explicitly authorized by the CA Manager and used by authorized and knowledgeable CA personnel?			
131	Are CA systems automatically terminated and interactive sessions re-authenticated after a determined period (e.g. 5 minutes) of inactivity?			
132	Does the CA ensure, to the extent possible, that no individual performs all aspects of the CA process?			
133	Are CA employees with privileged access trained and their activities monitored to ensure the appropriate security is maintained during their periods of access?			
134	Have redundant hardware, software, and communications components been implemented as part of the CA availability mechanisms?			
135	Do back-up systems automatically switch the required hardware, software, and communications components to primary status upon failure of the primary CA system?			

Detection and Surveillance

Item	Activities	Yes	No	Comments
136	Are CA system logs being checked at randomly selected periods to verify that all processes were authorized?			

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX – 10 SECURITY POLICY INDEX

The following is a list of Information Technology Security Policy Statements that must be addressed in a Certification Authority's CA policy to enter into a Cross-certification arrangement with the CCF. An example of an ITS Policy may be obtained at http://.

- Introduction
    - Policy Objective
    - Policy Statement
    - Application
    - Accountability
- Policy Requirements
    - CA Organization
    - Risk Management Process
    - Contingency Planning
    - Awareness and Training
    - Job Descriptions
    - Operating Procedures
    - Monitoring
    - Reviews
    - Inspections
    - Breaches and Violations
    - Personnel Security
        - CA Privileged Users
        - Local Registration Authorities
        - Subscribers
        - Segregation of Responsibilities
    - Information Security Policy
        - Information Labeling
        - Safeguarding of Information
        - Backups
        - Audit Logs
        - Archives
        - Disposal of Information
    - Physical Security
        - CA Facilities
        - Local Registration Authorities Facilities
    - Hardware and Software Security
        - Configuration Management
        - Connectivity
        - Communications
        - Software Components
        - Hardware Components
        - System Privileges
    - Operational Security
- Policy Revisions

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 11 - SECURITY PROCEDURES INDEX

The following is a list of information technology security procedures that must be addresses to enter into a cross-certification arrangement with the CCF. An example of ITS procedures may be obtained at http://.

Hierarchy of CA Policies and Procedures

Physical and Environmental Security Procedures

Security Incident Reporting

Personnel Security Procedures

IT Security Roles and Responsibilities

Procedural Security Practices

Handling and Storage of IT Media
Monitoring and Reviewing Privileged Access
Configuration Management Procedures
Problem Management Procedures
Change Management Procedures

Security Event Monitoring, Logging, and Incident Handling Procedures

Audit and Security Review Procedures

Technical Security Procedures

Master User Functions
Security Officers Functions
Administrators Functions
Key Management
Backup and Restore
Account Management
Power-up/Power-down and Startup and Shutdown
Certification Revocation and Key Recovery

CA Organization Chart

Maintenance Procedures

PROTECTED "A"
(when completed)

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 12 - COMPLIANCE INSPECTION CHECKLIST

Institution Name:	Address:
Name of Candidate CA participants:	Registration Number:
Name of Negotiation Team Members:	Date: Date of any previous Inspections:
GOC PKI CP Level requested by Candidate CA.	Is this entity internal or external to the GOC PKI? □ Internal □ External

Item	Question	Answer
ADMINISTRATIVE PRE-REQUISITES		
1	Has the CA submitted an application to the Policy Management Authority (PMA) to cross certify with the GoC PKI?	Yes No
	Was a Decision to Proceed Granted?	Yes No
	Do you have a representative of your organization on the PMA?(see PKI policy)	Yes No
2	Has the CA published a Certification Practice Statement (CPS)?	Yes No
	Which Certificate Policies (CPs) has the Certification Authority (CA) adopted?	a) GoC CP b) Departmental/organizational CP c) Other
	Have the CPs been mapped to the GoC CPs?	Yes No
	If so, has a summary report been provided to the Cross-Certification Team?	

Item	Question	Answer
	Has the CA cross-certified with any other CAs?	Yes No This question does not appear to have been asked in Phase I
3	Were policies defined in your CP intended for use by your department and/or organization only?	Yes No
1.1 OVERVIEW (GOC PKI CP)		
	Does your policy state that the issuance of a public key certificate does not imply that a Subscriber has any authority to conduct business transactions on behalf of the organization operating the CA?	This sort of statement should be incorporated into the Subscriber agreement
1.1.1 Policy Overview		
6	What is the CA's Policy Object Identifier Designation for its CPs?	
	Where cross-certificates have been issued, does the CA inform Subscribers which applications are intended to be used with the GoC PKI system?	Yes No
	Does the CA ensure that it associates itself and uses one Certificate and one CRL repository for each type of certificate?	
	Are Digital signature keys backed up or otherwise stored?	Yes No
	Has personal information collected by a CA ever been disclosed without the Subscriber's consent? If so, it was required by law?	Yes No
8	Are certificates made available to Subscribers before or after publication?	
	Is there a vehicle for Subscribers to correct information contained in a published certificate?	Yes No
	How are disputes concerning key or certificate management resolved under this policy?	
9	What maximum dollar amount is permitted per instance of use?	$0 Up to $5000 Up to $50000 Up to 1000000 Other (specify)
1.3.1 Certification Authorities (CAS)		

Item	Question	Answer
10	For which of the following is your CA responsible?	Creating and signing certificates binding Subscribers with their signature verification keys – Creating and signing certificates binding Subscribers with their public encryption keys – Creation and signing of certificates binding Subscribers, PKI personnel and (where permitted) other CAs with their signature verifications keys? – Creation and signing of certificates binding Subscribers and PKI personnel with their public encryption key? – Creation of End-Entity Confidentiality key pairs (if required)? (Same as subscriber encryption key pairs) – Promulgating certificate status through Certificate Revocation Lists (CRLs)? – Ensuring adherence to its CP?
11	If a department and/or organization has chosen to use a contractor to provide CA services, does the department and/or organization assume responsibility and accountability for the operation of its CA?	Yes No
	Is there a contract or other written arrangement?	Yes No
12	Has the CA cross-certified with any other CA?	Yes No
13	If cross-certified with any other CAs are agreements made with other CAs documented?	Yes No N/A
14	If cross-certified with any other CAs, are applicable disclaimers made available to Subscribers?	Yes No N/A
	1.3.2 Local Registration Authorities (LRAs)	
	Has your CA established LRAs? If so, how many?	Yes How many? No
	Has the CA assigned specific responsibilities to the LRA?	Yes No
15	How do you ensure that LRAs operating under your Certificate Policy are responsible for all duties assigned to them by the CA?	

Item	Question	Answer
	What is the relationship between the CA and the LRAs?	Same department Other department by MOU Private entity by contract Agent other
	Has the CA ensured that the LRA satisfies all the requirements of the CP?	Yes No
	1.3.3 Repositories	
17	Does the CA have at least one certificate and Certificate Revocation List repository associated with it?	Yes No
18	Is the repository in the form of one or more directories that comply with the Government of Canada (GoC) X.500 standards profile?	Yes No If no, state the form of the repository?
19	If the repository is not under the control of a CA, which of the following terms and conditions of its association does the CA included:	• Subjects of availability? • Access control? • Integrity of data? • Directory replication? Directory chaining? Other N/A
	1.3.4 Subscribers	
	Is responsibility and accountability attributable to an individual or an organization for certificates, which are issued to Subscribers?	Yes No
	Are PKI certificates only issued after authorization from one or more sponsors?	Yes No
	Is eligibility for a certificate at the sole discretion of the CA?	Yes No
	1.3.6 Policy Applicability	
	Are the certificates intended to be used to protect designated (insert GSP definition of designated) information?	Yes No
	If yes to the above, what consequences could be expected if the information was compromised?	Explain N/A
	1.3.6.1 Approved and prohibited applications	
22	A CA must advise Subscribers which applications are to be used with the PKI system. Are these applications, as a minimum, meeting the following requirements:	
	Does the PKI correctly establish, transfer and using the public and private keys?	Yes No
	Is it capable of performing the appropriate certificate validity and verification checking?	Yes No

Item	Question	Answer
	Does it reporting appropriate information and warnings to the Subscribers?	Yes No
23	Does the CA operate in accordance with the following when issuing and managing the keys provided to LRAs and Subscribers: • CPS? • CP? • Applicable Laws	Yes No, explain:
24	Does the CA verify the activities of the LRA to ensure that it is compliant to the CP requirements?	Yes No
25	Does the CA make Subscribers aware of their rights and obligations with respect to the operation and management of the following when used in connection with the PKI: • Keys? • Certificates? • End-Entity hardware? • End-Entity software?	Yes No
	If so, how?	
26	Does the CA do each the following: • Issue a CPS? • What mechanisms and procedures are in place to ensure that its LRAs and Subscribers are aware of, and agree to abide with, the stipulations of the CP that applies to them? • Establish that any CA with whom it cross-certifies complies with all CPs that are mutually recognized? • Through compliance inspection, verify to cross-certifying CAs that it complies with its CP?	
27	Are the CA personnel associated with the following PKI roles individually accountable for transactions they perform: • PKI Administrators? • PKI Master Users? • PKI Officers?	Yes No
	2.1.1.1 Notification of certificate issuance and revocation	
29	How does the CA make CRLs available to Subscribers or relying parties?	
30	Does the CA notify a Subscriber when a certificate bearing the Subscriber's DN is issued or revoked?	Yes No

Item	Question	Answer
	2.1.1.2 Accuracy of representations	
31	Has the CA certified that the information stated in a certificate issued to a Subscriber was verified in accordance with its CP prior to publishing the certificate in a repository to which the subscriber has access?	Yes No
32	Has the CA provided each Subscriber with notice of the Subscriber's rights and obligations under its CP?	Yes No
33	What are: • The allowed uses of the certificates issued under the CP? • The Subscriber's obligations concerning key protection? • Procedures for communication between the Subscriber and the CA or LRA?	
35	Describe the Relying Party's obligations with respect to the following: • Use of certificates? • Verification of certificates? • Validation of certificates?	
37	Does your policy ensure that the period for which the Entity has to complete its initialization process? If so what is the prescribed time allowed?	• – no stipulation? • – five working days? • – two working days? • – immediately?
	2.1.1.4 Certificate revocation and renewal	
38	Do procedures for the expiration, revocation and re-issuance of a certificate conform to the relevant provisions of the CP? NOTE: Not applicable for Rudimentary	Yes No N/A
39	Are the certificate revocation and renewal procedures expressly stated in the CPS, the Subscriber Agreement or any other applicable document outlining the terms and conditions of the certificate use? NOTE: Not applicable for Rudimentary	Yes No N/A
41	Is the location of the CRL defined in the certificate? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
2.1.1.5 Protection of private keys		
42	Has the CA ensured that the private keys that it holds or stores, and the activation data are protected in the CA encrypted database?	Yes No
43	Does the CP require that all entities protect their private keys and activation data in accordance with departmental and/or organizational policy?	Yes No
44	Has the CA ensured that any Confidentiality private keys of a Subscriber that have been backed- up or archived are protected?	Yes No
	How?	
45	Does the CA have a policy of non-disclosure of private keys?	Yes No
2.1.1.6 Restrictions on issuing CA's private keys		
46	Has the CA ensured that its certificate signing private key is used only to sign certificates and CRLs?	Yes No
48	Has the CA ensured that private keys issued to its personnel to access and operate CA applications are used only for such purposes?	Yes No
2.1.2 LRA obligations		
50	Has the CA ensured that all its LRAs comply with all the relevant provisions of the CA's CP and the CA's CPS? NOTE: Not applicable for Rudimentary	Yes No
51	Is the CA responsible through its LRAs to bring to the attention of Subscribers all relevant information pertaining to the rights and obligations of the CA, LRA, and Subscriber contained in the following: • CP? • CPS? • Subscriber agreement (if applicable)? • Any other relevant document outlining the terms and conditions of use? NOTE: Not applicable for Rudimentary	Yes No N/A
52	Do records of all transactions carried out in performance of LRA duties identify the individual who performed the particular duty? NOTE: Not applicable for Rudimentary	Yes No N/A
53	Are LRA Administrators individually accountable for transactions performed on behalf of the CA? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
55	When the LRA submits Subscriber information to the CA, does the LRA certify to the CA that it has authenticated the identity of that Subscriber? NOTE: Not applicable for Rudimentary	Yes No N/A
56	When performing LRA duties on-line through a remote administration application with the CA, do LRAs ensure that their private keys are protected? NOTE: Not applicable for Rudimentary	Yes No N/A
57	Are private keys used by LRAs to access and operate on-line LRA applications used for any other purpose? NOTE: Not applicable for Rudimentary	Yes No N/A
	2.1.3 Subscriber obligations	
58	Has the CA ensured that a Subscriber enters into an agreement or abides by an agreement by an acceptable use policy which outlines the terms and conditions of use, including permitted applications and purposes?	Yes No
	2.1.3.1 Representations	
59	Does the CA require that information submitted in connection with a certificate be complete and accurate?	Yes No
60	What proportion of every 24-hour period is the repository available?	
61	What is the availability of certificates and CRLs to Relying Parties?	no stipulation? 24 hours? 12 hours? 4 hours? Other?

Item	Question	Answer
	2.2 LIABILITY	
	2.2.1 Requirements	
62	Has the CA ensured that the following are in accordance with its CP: • Certification and repository services? • Issuance and revocation of certificates? • Issuance of CRL? • CA and LRA obligations are implemented and comply with authentication and validation procedures?	Yes No
64	Do you have a Disclaimer of warranties and obligations policy?	Yes No
	What is the substance of the Disclaimer?	
	2.2.3 Limitations of liability	
65	• Do you limit liability and if so, please elaborate.	• no stipulation? • $5,000 per instance? • $50,000 per instance? • $1,000.000 per instance?
	2.2.4 Other terms and conditions	
66	Are disclaimers or limitations of liability contained in the CPS consistent with the CP?	Yes No
	2.3 FINANCIAL RESPONSIBILITY	
67	Has the CA contracted for the provision of its CA services?	Yes No
68	If so, did the CA ensure that the contracted CA provided the following: • Satisfactory evidence of financial responsibility? • Waiver of any legislative immunity (if applicable)?	Yes No N/A
	2.4 INTERPRETATION AND ENFORCEMENT	
	2.4.1 Governing law	
69	What laws govern the CA? •	

Item	Question	Answer
	2.4.2 Severability, survival merger, notice	
70	Do agreements entered into by the CA contain appropriate provisions governing the following: • Severability? • Survival? • Merger? • Notice?	Yes No
	2.4.3 Dispute resolution procedures	
71	Do agreements that the CA has entered contain provisions for appropriate dispute resolution procedures?	Yes No
	2.5 FEES	
72	Does the CA charge fees, and if so, how much and for what? How does the CA notify Subscribers?	Yes No Explain
	2.6 PUBLICATION & REPOSITORY	
73	Has the CA included within any certificate it issues the URL of a web site maintained by, or on behalf, of the CA?	Yes No
74	Does the CA ensure the publication of its CP and its CPS, digitally signed by an authorized representative of the CA, on a Web site maintained by, or on behalf, of the CA?	Yes No
75	Has the CA ensured, directly, or through agreement with a repository, that operating system and repository access controls are configured so that only authorized CA personnel can write or modify the online version of the CP and the CPS?	Yes No
77	Has the CA ensured, directly or with agreement with a repository, unrestricted access to CRLs?	Yes No

Item	Question	Answer
	2.7 COMPLIANCE INSPECTION	
	2.7.1 Frequency of Compliance Inspection	
79	Have Compliance Inspections been conducted prior to the initial cross certification with GoC PKI? Have Compliance Inspections been conducted as a minimum? for the following assurance levels:	Yes No • - every 3 years? • – every 2 years? • – every 12 months?
	2.7.2 Identity/qualifications of CA Inspector	
80	Who appoints the Inspectors?	
81	Are Inspections performed by a person with significant experience with the following: • PKI? • Cryptographic technologies? • Operation of relevant PKI software?	Yes No
	2.7.3 Inspector's relationship to audited CA	
82	Is the Inspector independent of the CA?	Yes No
83	Does the Inspector comply with the following:	Independent of the CA? Comply with the Conflict of Interest provisions?
2.7.4	**Topics covered by Inspection**	
84	Which topics are covered by the Inspection?	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 those technical, procedural and personnel practices and policies? The LRA, if used, implements those technical, procedural and personnel practices and policies set out by the CA?

Item	Question	Answer
	2.7.5 Actions taken as a result of inspection	
85	Are there procedures for taking action, where required?	Yes No
86	What provisions are in place to protect confidential, sensitive or personal information?	
	3.1 INITIAL REGISTRATION	
	3.1.1 Types of names	
87	Does each Entity have a clearly distinguishable and unique X.501 DN in the certificate subject name field and in accordance with PKIX Part 1? NOTE: Not applicable for Rudimentary	Yes No N/A
89	Is the DN in the form of an X.501 printable String and not left blank? NOTE: Not applicable for Rudimentary	Yes No N/A
	3.1.2 Need for names to be meaningful	
90	Do the contents of each certificate Subject and Issuer name fields have an association with the authenticated name of the Entity? NOTE: Not applicable for Rudimentary	Yes No N/A
91	In the case of individuals, is the Relative Distinguished Name (RDN) a combination of the following: • NOTE: Not applicable for Rudimentary	First name? Surname? Initials (Optional)? N/A
93	In the case of other entities, does the RDN reflect the authenticated legal name of the Entity? NOTE: Not applicable for Rudimentary	Yes No N/A
94	Where a certificate refers to a role or position, does the certificate also contain the identity of the person who holds that role or position? NOTE: Not applicable for Rudimentary	Yes No N/A
95	Where a certificate is issued for a device, does it include within the DN, the name of the person or organization responsible for the device? NOTE: Not applicable for Rudimentary	Yes No N/A
	3.1.4 Uniqueness of names	
96	Are Distinguished Names unique for all End-entities of a CA?	Yes No

Item	Question	Answer
3.1.5 Name claim dispute resolution procedure		
98	Does the CA reserve the right to make all decisions regarding Entity names in all assigned certificates?	Yes No
100	Where there is a dispute about a name in a repository not under the CA's control, does the CA ensure that there is a name claim dispute resolution procedure in its agreement with that repository?	Yes No
3.1.7 Method to prove possession of private key		
101	Do the issuing CA and End-entity confirm their respective identities through the use of a shared secret prior to the issuance of a verification certificate? NOTE: Not applicable for Rudimentary	Yes No If no, what other method is used:
102	Do the Issuing CA and End-entity confirm their respective identities through the use of a shared secret prior to the exchange of a private decryption key? NOTE: Not applicable for Rudimentary	Yes No If no, what other method is used:
3.1.8 Authentication of organization identity		
	How is the identification of a prospective Subscriber verified?	The CA or LRA examines notarized copies of documentation providing evidence of the existence of the organization? Other, specify:
104	Where the technology does not permit the independent generation of Digital Signature and Confidentiality key pairs, is the Digital Signature key pair used?	Yes No
105	If not, is the Digital Signature key pair used to provide certificates for use by organizations?	Yes No
106	Is the authority verified of the individual representing the prospective Subscriber?	Yes No
108	Does the CA or LRA verify the identity and authority of the individual acting on behalf of the prospective Subscriber and his/her authority to receive the keys on behalf of that organization?	Yes No
109	Does the CA or LRA keep a record of the type and details of identification used?	Yes No

Item	Question	Answer
	3.1.9 Authentication of individual identity	
111	How is the identification and authentication of individuals making an application for an individual to be a Subscriber established?:	
	3.1.10 Authentication of devices or applications	
113	How was the identification and authentication of the applicant verified? NOTE: Not applicable for Rudimentary	Explain N/A
114	Did the CA or LRA also verify the identity of the individual or organization making the application and their authority to receive the keys for that device or application? NOTE: Not applicable for Rudimentary	Yes No N/A
	3.2 AUTHENTICATION FOR ROUTINE REKEY	
116	Does the CA authenticate all requests for re-key?	Yes No
117	Does the Entity authenticate the subsequent response?	Yes No
118	Is the authentication done by an on-line method in accordance with PKIX Part 3 – Certificate Management Protocol?	Yes No
120	Where one of the keys has expired, is the request for re-key authenticated in the same manner as for initial registration?	Yes No
	3.3 AUTHENTICATION FOR REKEY AFTER REVOCATION	
121	Does the CA authenticate a re-key in the same manner as for initial registration where there is a known or suspected compromise of the private key?	Yes No
122	Does the CA or LRA authorized to act on behalf of the CA verify any change in the authentication information contained in a certificate?	Yes No
	3.4 AUTHENTICATION OF REVOCATION REQUEST	
123	Does the CA, or LRA acting on its behalf, authenticate a request for revocation of a certificate?	Yes No

Item	Question	Answer
124	Does the CA 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?	Yes No
125	Does the CA or LRA log requests for revocation of certificates?	Yes No
	4.1 APPLICATION FOR A CERTIFICATE	
126	Does the CA ensure that all procedures and requirements with respect to an application for a certificate are established and published in the CPS or a publicly available document?	Yes No
127	Are bulk applications on behalf of End-Entities permitted only by such persons authorized to make such applications? NOTE: Not applicable for Rudimentary	Yes No
128	Which of the following must accompany each application?:	Proof of the End-entity's identity? Proof of authorization for any requested certificate attributes? A signed agreement, or for employees, an acknowledgement of the applicable terms and conditions governing their use of the certificate? A public verification key generated by the end-entity?
	4.3 CERTIFICATE ACCEPTANCE	
129	Does the CA ensure that an Entity acknowledges acceptance of a certificate?	Yes No
130	In the case of a device or application, does the CA ensure that the individual or organization responsible for that device or application does the acknowledgement?	Yes No

Item	Question	Answer
	4.4 CERTIFICATE SUSPENSION & REVOCATION	
	4.4.1 Circumstances for revocation	
131	Does the CA revoke certificates for the following: • 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? • At the CA's discretion, when the Entity fails to comply with obligations set out in its CP, the CPS, any agreement or any applicable law?	Always Only if cross-certified
	4.4.3 Procedure for revocation request	
133	Are all procedures and requirements with respect to the revocation of a certificate set out in the CPS or otherwise made publicly available? NOTE: Not applicable for Rudimentary	Yes No N/A
134	Does the CA record and retain authenticated revocation requests and any resulting actions taken by the CA? NOTE: Not applicable for Rudimentary	Yes No N/A
135	In the case where a certificate is revoked, is a description of the reason for the revocation documented? NOTE: Not applicable for Rudimentary	Yes No N/A
136	Is the revocation of an Entity certificate published in the appropriate CRL? NOTE: Not applicable for Rudimentary	Yes No N/A
	4.4.4 Revocation request grace period	
137	Specify the period of time within which action is taken as a result of a request initiated for the revocation of a certificate	no stipulation? 24 hours? 12 hours?immediately?
	4.4.9 CRL issuance frequency	
138	Specify the frequency for which the CA issues an up to date CRL:	no stipulation? 24 hours? 12 hours? 4 hours?

Item	Question	Answer
139	Is the CA's CRL issuance synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to Relying Parties? NOTE: Not applicable for Rudimentary	Yes No N/A
140	Is an updated CRL issued immediately upon a certificate being revoked due to key compromise? NOTE: Not applicable for Rudimentary	Yes No N/A
4.4.15 Special requirements regarding key compromise		
141	In the event of the compromise, or suspected compromise of the CA signing key, does the CA notify immediately all CAs to whom it has issued cross-certificate (e.g. CCF) and the PMA?	Yes No
142	In the event of the compromise or suspected compromise, of any other Entity's signing key, and/or Entity's decryption private key, does the Entity notify the issuing CA immediately? NOTE: Not applicable for Rudimentary	Yes No N/A
143	Does the CA 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? NOTE: Not applicable for Rudimentary	Yes No N/A
4.5 SYSTEM SECURITY AUDIT PROCEDURES		
4.5.1 Types of event recorded		
147	Does the CPS indicate what information is logged? Please elaborate. NOTE: Not applicable for Rudimentary	Yes No.
4.5.2 Frequency of audit log processing		
149	With what frequency does the CA ensure that its audit logs are reviewed:	There is no stipulation? Every 2 weeks? Every week? daily?
150	Are all significant events explained in a audit log summary? NOTE: Note applicable for Rudimentary	Yes No N/A
151	Are actions taken from these reviews documented? NOTE: Note applicable for Rudimentary	Yes no

Item	Question	Answer
	4.5.3 Retention period for audit log	
152	How long does the CA retain its audit logs onsite? Are they subsequently archived? NOTE: Note applicable for Rudimentary	How long: N/A Yes No N/A
	4.5.4 Protection of audit log	
153	Does the electronic audit log system include mechanisms to protect the log files from unauthorized viewing, modification, and deletion? NOTE: Note applicable for Rudimentary	Yes No N/A
154	Is manual audit information protected from unauthorized viewing, modification and destruction? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.5.5 Audit log backup procedures	
155	Are audit logs and audit summaries backed up or copied if in manual form? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.5.6 Audit collection system	
156	Are audit collection systems identified in the CPS? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.5.8 Vulnerability assessments	
158	Events in the audit process are logged, in part, to monitor system vulnerabilities. Does the CA ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.6 RECORDS ARCHIVAL	
159	Are Digital Signature certificates, Confidentiality private keys stored by the CA, and ARLs and CRLs generated by the CA retained for at least one year after the expiration of the key material? NOTE: Note applicable for Rudimentary	Yes No N/A

Item	Question	Answer
160	Are audit information, subscriber agreements and any identification and authentication information retained for at least (6) years? NOTE: Note applicable for Rudimentary	Yes No N/A
161	Are backed up CA Confidentiality private keys protected at a level of physical and cryptographic protection equal to or exceeding that in place at the CA site? NOTE: Note applicable for Rudimentary	Yes No N/A
162	Is a second copy of all retained or backed up material stored in a location other than the CA site and protected either by physical security alone, or a combination of physical and cryptographic protection? NOTE: Note applicable for Rudimentary	Yes No N/A
163	Does the secondary site provide adequate protection from environmental threats such as temperature, humidity and magnetism? NOTE: Note applicable for Rudimentary	Yes No N/A
164	Is material stored off-site periodically verified for integrity? (CP suggests every 6 months) NOTE: Note applicable for Rudimentary	Yes No N/A
4.7 KEY CHANGEOVER		
166	Does the CPS include the details of the process for a Subscriber's renewal of a key pair and key changeover process? NOTE: Note applicable for Rudimentary	Yes No N/A
167	Does the CA or LRA re-authenticate Subscribers without valid keys in the same manner as the initial registration? NOTE: Note applicable for Rudimentary	Yes No N/A
168	Where a Subscriber's certificate has been revoked as a result of non-compliance, does the CA verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance? NOTE: Note applicable for Rudimentary	Yes No N/A
4.8 COMPROMISE AND DISASTER RECOVERY		
4.8.1 Computing resources, software, and/or data are corrupted		
170	Are business continuity procedures, which outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data established? NOTE: Note applicable for Rudimentary	Yes No N/A

Item	Question	Answer
171	Did the CA ensure that any agreement with a repository not under the control of the CA, provides that business continuity procedures be established and documented by the repository? NOTE: Note applicable for Rudimentary	Yes No N/A
4.8.2 Entity public certificate is revoked		
172	In the event of a need for revocation of a CA's Digital Signature certificate, does the CA immediately notify the following: NOTE: Note applicable for Rudimentary	PMA? (next business day) All CAs to whom it has issued cross-certificates? (CCF only?) All of its LRAs?(through departmental channels) All Subscribers?(end entities & organizations) All individuals or organizations who are responsible for a certificate used by a device or application?(not mentioned) N/A
173	Does the CA publish the certificate serial number on an appropriate CRL and revoke all cross-certificates signed with the revoked Digital Signature certificate? NOTE: Note applicable for Rudimentary	Yes No N/A
4.8.2.1 Entity public key is downgraded		
174	If a CA's Digital Signature certificate is downgraded, does the CA immediately notify the following: NOTE: Note applicable for Rudimentary	PMA?(next business day) All CAs to whom it has issued cross-certificates?(CCF) All of its LRAs?(through departmental channels) All Subscribers?(end entities and organizations) All individuals or organizations who are responsible for a certificate used by a device or application?(does not mention) N/A

Item	Question	Answer
175	Prior to re-establishing cross-certification, does the CA do the following: NOTE: Note applicable for Rudimentary	Request revocation of cross-certificates issued to the CA? Revoke all certificates signed with the higher assurance key? Provide appropriate notice? Generate a new CA signing key pair? Re-issue certificates to all Entities? Ensure that all CRLs and ARLs are signed using the new key?
176	In the event of a downgrade of any other Entity's Confidentiality certificate, does the CA or LRA notify the subscriber in a manner set out in its CPS and the Subscriber agreement? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.8.3 Entity key is compromised	
177	In the event of the compromise of a CA's Digital Signature key, does the CA do the followings prior to re-certification: NOTE: Note applicable for Rudimentary	• Request revocation of cross-certificates issued to the CA? • Revoke all certificates issued using that key? • Provide appropriate notice?
178	Does the CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise for the following keys: • Entity's Digital Signature key? • Entity's decryption private key? NOTE: Note applicable for Rudimentary	Yes No N/A
179	Does the CA notify the PMA immediately in the event of the compromise, or suspected compromise of a CA decryption private key? NOTE: Note applicable for Rudimentary	Yes No N/A
	4.8.4 Secure facility after a natural or other type of disaster	
180	Did the CA establish a disaster recovery plan, which outlines the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster? NOTE: Note applicable for Rudimentary	Yes No N/A
181	Where a repository is not under the control of the CA, did the CA ensure that any agreement with the repository provides that a disaster recovery plan is established and documented by the repository? NOTE: Note applicable for Rudimentary	Yes No N/A?

Item	Question	Answer
	4.9 CA TERMINATION	
182	In the event that a CA ceases operation, does the CA notify its Subscribers and all the CAs with whom it is cross-certified immediately upon termination of operations and arrange for the continued retention of the CA's keys and information? NOTE: Note applicable for Rudimentary	Yes No N/A
183	In the event of a change in management of the CA's operations, does the CA notify all Entities for which it has issued certificates and CAs with whom it has cross-certified? NOTE: Note applicable for Rudimentary	Yes No N/A
184	In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance, are the certificates issued by that CA, whose operations are being transferred, revoked through a CRL signed by that CA prior to the transfer? NOTE: Note applicable for Rudimentary	Yes No N/A
5.1 PHYSICAL CONTROLS		
	5.1.1 Site location, construction and physical access	
186	Is the CA located in a Reception zone? (if unknown, answer the following) Is the CA located at the entry to the facility where initial contact between the public and the department occurs, where services are provided, information is exchanged and access to restricted areas is controlled? To varying degrees, is activity in this area monitored by the personnel who work there, by other personnel or by security staff? Is access by the public limited to specific times of the day or for specific reasons? Is entry to the area indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment?	Yes No
	Is the CA located in an Operations Zone? (if unknown, answer the following?) Is the area to which access is limited to personnel and to properly-escorted visitors? Is the area monitored at least periodically, based on a TRA,? Is the area accessible from a Reception zone?	Yes No

Item	Question	Answer
	Is the CA located in a Security Zone? (if unknown, answer the following?) Is the CA in an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors? Is the area access from an Operations zone and through an entry point? Is the Area monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means?	Yes No
	Is the CA located in a High-Security Zone? (if unknown, answer the following) Is the CA in an area to which access is controlled through an entry point and limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors? Is the area accessible only from a Security Zone and separated from Security Zones and Operations Zone by a perimeter built to the specifications recommended in the TRA? Is the area monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means?	Yes No
187	Is the CA site manually or electronically monitored for unauthorized intrusion?	At all times No Some of the time (specify)
188	Is unescorted access to the CA server limited to those personnel identified on an access list?	Yes No
189	Are personnel not on the access list, properly escorted and supervised?	Yes No
190	Is a site access log maintained and audited periodically?	Yes No
191	Are all removable media and paper containing sensitive plain text information stored in containers either listed in, or of equivalent strength to those listed in, the Security Equipment Guide?	Yes No
192	Are all LRAs located in an area that satisfies the controls required for a Reception Zone?	Yes No

Item	Question	Answer
193	If an LRA workstation is used for on-line Entity management with the CA, is the workstation located in one of the following zones:	Operations Zone OR a Reception Zone with all media security protected when unattended? A Security Zone OR a Operations Zone while attended with all media security protected when unattended? N/A
194	Has the CA ensured that there is appropriate security protection for the following and how: • Cryptographic module? • All system software? • The LRA Administrator's Private key?	Yes No Explain:
195	Does the CA ensure, by a TRA, that the operations of the LRA site provides appropriate security protection of the cryptographic module, all system software and the LRA Administrator's private key?	Yes No
196	Are recorded PINs and passwords stored in a security container accessible only to authorized personnel?	Yes No
197		Rhonda Lazarus notes that this question cannot be answered by a CA.
198	Is the hard drive on a workstation containing private keys physically secured or protected with an appropriate access control product?	Yes No
199	Is the Subscribers hardware cryptographic module physically protected by the following: • Through site protection? • Being kept with the Subscriber? NOTE: for High Assurance only	Yes No N/A
	5.1.3 Power and air conditioning	
200	Did the CA ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system? NOTE: Not applicable for Rudimentary	Yes No N/A
	5.1.4 Water exposures	
201	Has the CA ensured that the CA system is protected from water exposure? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
	5.1.5 Fire prevention and protection	
202	Has the CA ensured that the CA system is protected with a fire suppression system? NOTE: Not applicable for Rudimentary	Yes No N/A
	5.1.6 Media storage	
203	Has the CA ensured that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism? NOTE: Not applicable for Rudimentary	Yes No N/A
	5.1.7 Waste disposal	
204	Has all media used for the storage of sensitive information such as keys, activation data or CA files been sanitized or destroyed before release for disposal? NOTE: Not applicable for Rudimentary	Yes No N/A
	5.1.8 Off-site backup	
205	Does the CA have off-site backup facilities? NOTE: Not applicable for Rudimentary	- - Yes - No - N/A
206	Do these off-site backup facilities have the same level of security as the primary CA site? NOTE: Not applicable for Rudimentary	Yes No N/A
	5.2.1.1 CA Trusted Roles	
207	Does the CA ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection?	Yes No (if no go to question 215)
208	Is each user's system access limited to those actions for which they are responsible to perform in fulfilling their responsibilities?	Yes No N/A
213	If an alternative division of responsibilities is used, does it provide the same degree of resistance to insider attack?	Yes No Explain N/A

Item	Question	Answer
5.2.1.2 LRA Trusted Roles		
215	Does the CA 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 request? • 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? NOTE: Not applicable for Rudimentary	Yes No
5.2.2 Number of persons required per task		
218	Does the key recovery operation require a minimum of two individuals using a split knowledge technique such as twin passwords? NOTE: Not applicable for Rudimentary	yes no N/A
220	Is multi-user control exercised for CA key generation? NOTE: Not applicable for Rudimentary	Yes No N/A
221	Does the CA ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders? NOTE: Not applicable for Rudimentary	Yes No N/A
5.2.3 Identification & Authentication for each role		
222	Did all CA personnel have their identity and authorization verified for the following activities: • Before being included in the access list for the CA site? • Before being included in the access list for physical access to the CA system? • Before being given a certificate for the performance of their CA role? • Before being given an account on the PKI system? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
223	Does each certificate and account (with the exception of CA signing certificates) meet the following standards: • Directly attributable to an individual? • Not shared? • Restricted to actions authorized for that role through the use of CA software, operating system and procedural controls? NOTE: Not applicable for Rudimentary	Yes No N/A
224	Are CA operations secured using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network? NOTE: Not applicable for Rudimentary	Yes No N/A
5.3 PERSONNEL SECURITY CONTROLS		
225	Have all personnel performing duties with respect to the operation of a CA or LRA been: • Appointed in writing? • Bound by contract or statute to the terms and conditions of the position they are to fill? • Received comprehensive training with respect to the duties they are to perform? • Bound by statute or contract not to divulge sensitive CA security-related information or Subscriber information? • Not assigned duties that may cause a conflict of interest with their CA or LRA duties?	Yes No
226	What security clearance Do all personnel performing duties with respect to the operation of a CA hold	Enhanced Reliability Check Level II (Secret) Other (specify)
227	Do all personnel who operate a LRA workstation for the purpose of on-line Entity management with the CA, hold an Enhanced Reliability Check? Does it include fingerprint check and a credit check?	Yes No Yes No
5.3.2 Background Check Procedures		
228	Have the background checks been performed in accordance with the Government Security Policy, or equivalent?	Yes no

Item	Question	Answer
229	Have the personnel performing duties with respect to the operation of a CA or LRA received comprehensive training in the following topics: • CA/LRA security principles and mechanisms? • All PKI software versions in use on the CA system? • All PKI duties they are expected to perform? • Disaster recovery and business continuity procedures?	Yes No
230	Are the training requirements with respect to the operation of a CA or LRA operation kept current to accommodate changes in the CA system?	Yes no
231	Refresher training must be conducted as required to accommodate changes in the CA system. Does the CA review these requirements at least once a year?	Yes No
	5.3.7 Contracting Personnel	
233	Does the CA ensure that contractors are properly escorted and supervised?	Yes No
234	Do all CA and LRA personnel have the following documentation available to them: • The certificate policies it supports? • It's CPS? • any specific statutes, policies or contracts relevant to their position?	Yes No
	6 TECHNICAL SECURITY CONTROLS	
	6.1 Key Pair Generation and Installation	
	6.1.1 Key Pair Generation	
235	Does each prospective certificate holder generate its own Digital signature key pair using a PMA approved algorithm? NOTE: Not applicable for Rudimentary	Yes No
236	Does each prospective certificate holder generate its own Confidentiality key pair using a PMA approved algorithm? NOTE: Not applicable for Rudimentary	Yes No

Item	Question	Answer
6.1.2 Private Key Delivery to Entity		
237	If the private decryption key is not generated by the prospective certificate holder, is it delivered to the Entity in one of the following ways: NOTE: Not applicable for Rudimentary	• An on-line transaction in accordance with IETF PKIX-3 Certificate Management Protocol? • Via an equally secure manner approved by the PMA? • Other, explain
6.1.3 Public Key Delivery to Certificate Issuer		
238	Is the public verification key delivered to the CA via one of the following ways: NOTE: Not applicable for Rudimentary	• An on-line transaction in accordance with the PKIX-3 Certificate Management Protocol? • Via an equally secure manner approved by the PMA? • Other, explain
239	If the public encryption key is not generated by the CA, is it delivered to the CA in one of the following ways: NOTE: Not applicable for Rudimentary	• An on-line transaction in accordance with the PKIX-3 Certificate Management Protocol? • Via an equally secure manner approved by the PMA? • Other, explain
6.1.4 CA Public Key Delivery to Users		
240	Is the CA public verification key delivered to the prospective certificate holder in one of the following ways: NOTE: Not applicable for Rudimentary	• An on-line transaction in accordance with PKIX-3 Certificate Management Protocol? • Via an equally secure manner approved by the PMA? • Other, explain
6.1.5 Asymmetric Key Sizes		
241	Which standards do key pairs for all PKI entities meet •	• 512 bit RSA or DSA? • 1024 bit RSA or DSA? • 2048 bit RSA?
6.1.6 Public key parameters generation		
242	Does the CA utilize the DSA algorithm that generate parameters in accordance with FIPS 186?	Yes No

Item	Question	Answer
	6.1.8 Hardware/Software Key Generation	
244	Is generation of Digital Signature keys for all Entities generated in a hardware cryptographic module for High Level Assurance? NOTE: For High Assurance only	Yes No N/A
245	Are CA Digital signature key pairs generated in a hardware cryptographic module for the following assurance levels: NOTE: Not applicable for Rudimentary	Yes No N/A
	6.1.9 Key Usage Purposes (as per X.509v3 field)	
247	Are CA signing keys the only keys permitted for signing certificates and CRLs? NOTE: Not applicable for Rudimentary	Yes No
248	Is the certificate key Usage field used in accordance with PKIX-1 Certificate Profile and CRL Profile? NOTE: Not applicable for Rudimentary	Yes No N/A
249	Are the following Key Usage values present in all certificates: • Digital Signature? • Non Repudiation? • Key Encipherment? • Data Encipherment? NOTE: Not applicable for Rudimentary	Yes No N/A
250	Are the following additional values present in CA certificate-signing certificates: NOTE: Not applicable for Rudimentary	• KeyCertSign? • CRLSign?
	6.2.2 Private Key Multi-person Control	
252	Is multiple person control exercised for CA key generation operations? NOTE: Not applicable for Rudimentary	Yes No N/A
253	Do two staff performing duties associated with the roles of PKI Master User or PKI Officer positions participate or are present for CA key generation operations? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
254	Is multiple person control exercised during private confidentiality key recovery? NOTE: Not applicable for Rudimentary	Yes No N/A
255	Do two staff performing duties associated with the roles of PKI Master User or PKI Officer or PKI Administrator positions participate or are present for private confidentiality key recovery? NOTE: Not applicable for Rudimentary	Yes No N/A
	6.2.3 Private Key Escrow	
256	Are Digital Signature Private keys ever escrowed?	Yes No N/A
	6.2.4 Private Key Backup	
257	Are backups of Digital Signature private key copied & stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key? NOTE: Not applicable for Rudimentary	Yes No N/A
259	Does the CA back up private keys? If so, are backed up private confidentiality keys copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key?	Yes No Yes No
	6.2.6 Private Key Entry into Cryptographic Module	
260	Are private decryption keys not generated by the Entity's cryptographic module entered into the following: NOTE: Not applicable for Rudimentary	• The module in accordance with PKIX-3 Certificate Management Protocol? • Via an equally secure manner approved by the PMA? Explain.
	6.2.7 Method of Activating Private Key	
261	Is the Entity authenticated (e.g. password) to the cryptographic module before activation of the private key? NOTE: Not applicable for Rudimentary	Yes No
262	Are deactivated private keys kept in encrypted form only? NOTE: Not applicable for Rudimentary	Yes No

Item	Question	Answer
	6.2.8 Method of Deactivating Private Key	
263	When keys are deactivated, are they cleared from memory before the memory is de-allocated? NOTE: Not applicable for Rudimentary	Yes No N/A
264	Is any disk space where keys were stored overwritten before the space is released to the operating system? NOTE: Not applicable for Rudimentary	Yes No N/A
265	Does the cryptographic module automatically deactivate the private key after a pre-set period of inactivity? NOTE: Not applicable for Rudimentary	Yes No N/A
	6.2.9 Method of Destroying Private Key	
266	Upon termination of use of a private key, are all copies of the private key in computer memory and shared disk space securely destroyed by overwriting? NOTE: Not applicable for Rudimentary	Yes No N/A
267	Is the method of overwriting approved by the PMA? NOTE: Not applicable for Rudimentary	Yes No N/A
268	Are private key destruction procedures described in the following documents: NOTE: Not applicable for Rudimentary	• CPS? • Subscriber agreement?
	6.3 Other Aspects of Key Pair Management	
	6.3.1 Public Key Archival	
269	Are all verification public keys retained by the issuing CA? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
	6.3.2 Usage Periods for the Public and Private Keys	
270	Do you have a validity period that meets the following minimum standards for the Digital Signature Key pair: • Rudimentary Level Assurance – ➢ one year without CRL? ➢ six years with CRL? • Basic Level Assurance – ➢ CA public verification key and certificate (six years)? ➢ CA private signing key (two years)? ➢ End-Entity public verification key and certificate (four years)? ➢ End-Entity private signing key (one year)? • Medium Level Assurance – ➢ (1024 bits key) - ♦ CA public verification key and certificate (two years)? ♦ CA private signing key (one year)? ♦ End-Entity public verification key and certificate (one year)? ♦ End-Entity private signing key (six months)? ➢ (2048 bits key) - ♦ 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)? • High Level Assurance – ➢ (2048 bits key) – ♦ 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)?	Yes No

Item	Question	Answer
271	Do you have a validity period that meets the following minimum standards for the Confidentiality Key pair: • Rudimentary Level Assurance – ➢ one year without CRL? ➢ six years with CRL? • Basic Level Assurance – ➢ CA public verification key and certificate (six years)? ➢ CA private signing key (two years)? ➢ End-Entity public encryption key and certificate (four years)? ➢ End-Entity private decryption key (no expiry)? • Medium Level Assurance – ➢ (1024 bits key) - ♦ CA public verification key and certificate (two years)? ♦ CA private signing key (one year)? ♦ End-Entity public encryption key and certificate (one year)? ♦ End-Entity private decryption key (no expiry)? ➢ (2048 bits key) - ♦ CA public verification key and certificate (twenty)? ♦ CA private signing key (eight years) ♦ End-Entity public encryption key and certificate (twelve years)? ♦ End-Entity private description key (no expiry)? • High Level Assurance – ➢ (2048 bits key) – ♦ 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 (no expiry)?	Yes No
6.4 Activation Data		
	Are activation data unique and unpredictable? NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
273	Does the activation data, in conjunction with any other access control, have an appropriate level of strength for the keys or data to be protected? NOTE: Not applicable for Rudimentary	Yes No N/A
274	Are the following codes protected from unauthorized use by a combination of cryptographic and physical access control mechanisms: • Data used for Entity initialization? • Private keys of Entities? NOTE: Not applicable for Rudimentary	Yes No N/A
275	Where passwords are used, does the entity have the capability to change its password at any time? NOTE: Not applicable for Rudimentary	Yes No N/A
276	Is the level of protection adequate to deter a motivated attacker with substantial resources? NOTE: Not applicable for Rudimentary	Yes No N/A
	6.5 Computer Security Controls	
	6.5.1 Specific Computer Security Technical Requirements	
280	Which of the following functionality does each CA server include (either provided by the operating system or through a combination of operating system, PKI CA software, and physical safeguards): NOTE: Not applicable for Rudimentary	• Access control to CA services and PKI roles? • Enforced separation of duties for PKI role? • Identification and authentication of PKI roles and associated identities? • Object Re-use or separations for CA random access memory? • Use of cryptography for session communication and database security? • Archival of CA and end entity history and inspection 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?

Item	Question	Answer
6.5.2 Computer Security Rating		
281	Did CSE, NSA or another accredited third party lab evaluate the security critical elements of the CA?	Yes No If not CSE or NSA, please include the name of the accredited third party.
282	Did the evaluation include system-level analysis?	Yes No
6.6 Life Cycle Technical Controls		
6.6.1 System Development Controls		
283	Does the CA use software that has been designed and developed under a development methodology such as MIL-STD-498, the system Security Engineering Capability Maturity Model (SSE CMM), or Information Security Engineering Handbook for the following assurance levels: NOTE: Not applicable for Rudimentary	Yes No If no, state the software used.
284	Did the design and development process provide sufficient documentation to support third party security evaluation of the CA components and be supported by third party verification of process compliance and ongoing Threat Risk Assessments to influence security safeguard design and minimize residual risk for the following assurance levels: NOTE: Not applicable for Rudimentary	Yes No
6.6.2 Security Management Controls		
285	Is a formal configuration management methodology used for installation and ongoing maintenance for the following assurance levels: • NOTE: Not applicable for Rudimentary	Yes No N/A

Item	Question	Answer
286	Does the CA software, when first loaded, provide a method for the Medium and High Level Assurances only CA to verify that the software on the system was: • Originated from the software developer? • Has not been modified prior to installation? • Is the version intended for use? NOTE: Not applicable for Rudimentary	Yes No N/A
287	Does the CA have a mechanism to periodically verify the integrity of the software? • NOTE: Not applicable for Rudimentary	Yes No N/A
288	Does the CA have mechanisms and policies in place to control and monitor the configuration of the CA system? • NOTE: Not applicable for Rudimentary	Yes No N/A
289	Was the integrity of the CA system validated upon installation? • At what frequency is the integrity of the CA system validated thereafter NOTE: Not applicable for Rudimentary	Yes No N/A Frequency:
6.7 Network Security Controls		
290	Is the CA server protected from attack through any open or general purpose network with which it is connected? NOTE: Not applicable for Rudimentary	Yes No N/A
291	Does the protection provided through the installation of a device (e.g. firewall) configured to allow only the protocols and commands required for the operation of the CA? NOTE: Not applicable for Rudimentary	Yes No N/A
292	Does the protection device (e.g. firewall) log all successful and unsuccessful attempts to communicate through to the CA components? NOTE: Not applicable for Rudimentary	Yes No N/A/

Item	Question	Answer
	6.8 Cryptographic Module Engineering Controls	
293	Are all CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations performed in the following : • Rudimentary Level Assurance – no stipulation? • Basic Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality and assurance? • Medium Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality and assurance? • High Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 3? ➢ Verified to an equivalent level of functionality and assurance?	Yes No

Item	Question	Answer
294	Are all other CA cryptographic operations performed in the following: • Rudimentary Level Assurance – no stipulation? • Basic Level Assurance - ➢ A cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality? • Medium Level Assurance - ➢ A cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality? • High Level Assurance - ➢ A cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality?	Yes No
295	Are the LRA Administrator Digital Signature key generation and signing operations performed in the following: • Rudimentary Level Assurance – no stipulation? • Basic Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • Medium Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • High Level Assurance - ➢ A hardware cryptographic module rated to at least FIPS-140-1 Level 2? ➢ Verified to an equivalent level of functionality and assurance?	Yes No

Item	Question	Answer
296	Are all other LRA cryptographic operations performed in the following: • Rudimentary Level Assurance – no stipulation? • Basic Level Assurance - ➢ A cryptographic module rated at FIPS 140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • Medium Level Assurance - ➢ A cryptographic modules rated at FIPS 140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • High Level Assurance - ➢ A cryptographic module rated at FIPS 140-1 Level 2? ➢ Verified to an equivalent level of functionality and assurance?	Yes no
297	Do end entities use cryptographic modules validated to at least the following standards: • Rudimentary Level Assurance – no stipulation? • Basic Level Assurance - ➢ FIPS-140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • Medium Level Assurance - ➢ FIPS-140-1 Level 1? ➢ Verified to an equivalent level of functionality and assurance? • High Level Assurance - ➢ FIPS-140-1 Level 2 ➢ Verified to an equivalent level of functionality and assurance?	Yes no
7 CERTIFICATE & CRL PROFILES		
7.1.1 Profile		

Item	Question	Answer
298	Does the CA issue X.509 Version 3 certificates in accordance with the PKIX Certificate and CRL Profile?	Yes No
299	Does the PKI End-Entity software support all the base (non-extension) X.509 fields as follows: • Signature – CA signature to authenticate certificate? • Issuer – name of CA? • Validity – activation & 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 the certificate, plus the certificate extensions?	Yes No
300	Does all entity PKI software correctly process the extensions identified in sections 4.2.1 and 4.2.2 of the PKIX certificate profile?	Yes No
301	Does the CPS define the use of any extensions supported by the CA, its LRA and End Entities?	Yes No
302	Is the "certificatePolicies" field set as critical in all of the certificates?	Yes No
	7.1.3 Algorithm object Ids	
303	What algorithms are used by the CA and supported by End Entities for certificate and object signing and verification? •	RSA 1024 in accordance with PKCS#1? RSA 2048 in accordance with PKCS#1? SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2)? Other?

Item	Question	Answer
304	Do the End-entities use the following algorithms for signing and verification: •	RSA 512 in accordance with PKCS#1? RSA 1024 in accordance with PKCS#1? RSA 2048 in accordance with PKCS#1? DSA in accordance with DSS (FIPS PUB 186) and ANSI X9.30 (Part 1)? MD5 in accordance with RFC-1321? SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2)?
7.1.4 Name Forms		
305	Is every DN in the form of an X.501 printableString? NOTE: Not applicable for Rudimentary	Yes No N/A
306	Do Subject and Issuer DNs meet the following: • Comply with PKIX standards? • Present in all certificates? NOTE: Not applicable for Rudimentary	Yes No N/A
7.1.6 Certificate policy object identifier		
307	Does the CA ensure that the policy OID is contained within the certificates it issues?	Yes No
7.1.7 Usage of policy constraints extension		
308	Are the Certificate Policy Constraints used in accordance with X.509v3?	Yes No
7.1.8 Policy qualifiers syntax and semantics		
309	Are Policy Qualifiers syntax in accordance with X.509v3?	Yes No
7.1.9 Processing semantics for the critical certificate policy		
310	Are critical extensions interpreted as defined in X.509v3?	Yes No

Item	Question	Answer
	7.2 CRL Profile	
	7.2.1 Version number	
311	Does the CA issue X.509 v2 CRLs in accordance with the PKIX Certificate and CRL Profile?	Yes No
312	Does all Entity PKI software correctly process all CRL extensions identified in the PKIX Certificate and CRL profile?	Yes No
313	Does the CPS define the use of any extensions supported by the CA, its LRAs and End Entities?	Yes No
	8 SPECIFICATION ADMINISTRATION	
	8.1.2 Changes with Notification	
314	Prior to making any changes to your certificate policy, does the CA notify the CCF and all CAs directly cross-certified with the CCF?	Yes No
8.1.2.1	**List of items**	
315	Are all items in the certificate policy subject to the notification requirement?	
	8.1.2.2 Notification Mechanism	
316	Does the CA notify all Subscribers of any proposed changes to the certificate policy?	Yes No
317	Is the notification in writing?	Yes No
318	Does the notification contain the following: • Statement of proposed changes? • Final date for receipt of comments? • The proposed effective date of change?	Yes No
319	Does the CA post a notice of the proposal on the CA Web site?	Yes No
	8.1.2.3 Comment Period	
320	Is the comment period 30 days unless otherwise specified?	Yes No
321	Is the comment period defined in the notification?	Yes No

Item	Question	Answer
	8.1.2.4 Mechanism to handle comments	
322	Are comments on proposed changes directed to the PMA?	Yes No
323	Are comments written and signed?	Yes No
	8.2 Publication & Notification Procedures	
327	Does the CA make an electronic copy of the CP and CPS, digitally signed by an authorized representative of the CA, available to its Subscribers and Relying Parties at the CA's Web site?	Yes No

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 13 - INFORMATION TECHNOLOGY SECURITY AND POLICY COMPLIANCE CERTIFICATE (CORPORATION)

TO: Her Majesty the Queen in right of Canada,
as represented by the President of the Treasury Board ("Canada")

RE: Request for Cross-certification with the Government of Canada Public Key Infrastructure

(or Cross-certification Agreement between .... ("the Corporation") and Canada dated..............................., section........ annual certification)

I, ..., hereby certify for and on behalf of the Corporation ....and to the best of my knowledge as follows:

1. I am the .... and a Director of the Corporation and have read the Request for Cross-certification (or relevant section of the Cross-certification Agreement) and made due inquiry, including having consultations with other officers, directors and employees of the Corporation and reviewing such documents as were necessary in order to give this certificate.

2. The Corporation acknowledges receipt of the following:
   a) Canada's Compliance Inspection Checklist and its Information Technology Security Evaluation Checklist;
   b) Canada's CP as at the date......; and
   c) Canada's CPS as at ....

3. The Corporation has completed, or has had completed by a qualified inspector, an inspection and evaluation according to the Checklists referred to in paragraph 2 (a) above. (or the following:
   a) an information technology security evaluation which accords substantively with Canada's ITS Evaluation Checklist;
   b) a compliance inspection which accords substantively with Canada's Compliance Inspection Checklist.)

4. The information technology security system of the Corporation's (PKI/CA) is accredited and certified (or approved) for and operates at a level of assurance (equivalent to Canada's Medium Assurance as defined in Canada's CP located at.... as at the date hereof.) (of...............................as described in the Corporation's CP and CPS.)

5. The Corporation's technical, physical, procedural, and personnel security policies and practices comply with the requirements of the Corporation's CP and CPS, and the Corporation has implemented and fully performs in accordance with the standards established in its CP and CPS.

6. Exceptions or qualifications:

This certificate is made with the knowledge that it will be relied upon by Canada.

This certificate shall remain in full force and effect and be binding upon the Corporation until a certificate repealing or replacing this certificate shall have been received by Canada and duly acknowledged in writing.

DATED at..this............day of................... , ...

----
signature of......................................, A.S.O.

INFORMATION TECHNOLOGY SECURITY AND POLICY COMPLIANCE CERTIFICATE

(Department)

TO: Her Majesty the Queen in right of Canada,
as represented by the President of the Treasury Board ("Canada")

RE: Request for Cross-certification with the Government of Canada Public Key Infrastructure (may have to specify which CA)

(or Memorandum of Understanding between .... (the "Department") and Canada dated..............................., annual certification ....Cross-certification Guidelines

I, ..., hereby certify for and on behalf of the Department ....and to the best of my knowledge as follows:

1. I am the (eg Security Officer)............ of the Department and have read the Request for Cross-certification (or relevant section of the Cross-certification Guidelines) and made due inquiry, including having consultations with other officers, employees and contractors of the Department and reviewing such documents as were necessary in order to give this certificate.

2. The Department acknowledges receipt of the following:
   a). Canada's Compliance Inspection Checklist and its Information Technology Security Evaluation Checklist;
   b) Canada's CP as at the date......;
   c) Canada's CPS as at ....

3. The Department has completed, or has had completed by a qualified inspector, an inspection and evaluation according to the Checklists referred to in paragraph 2(a) above. (or the following:
   a) an information technology security evaluation which accords substantively with Canada's ITS Evaluation Checklist;
   b) a compliance inspection which accords substantively with Canada's Compliance Inspection Checklist.)

4 The information technology security system of the Department's CA is accredited and certified (or approved) (pursuant to the Government Security Policy) for and operates at a level of assurance (equivalent to Canada's Medium Assurance as defined in Canada's CP located at.... as at the date hereof.)(of.......................described in the Department's CP and CPS.)

5. The Department's technical, physical, procedural, and personnel security policies and practices comply with the requirements of the Department's CP and CPS, and the Department has implemented and fully performs in accordance with the standards established in its CP and CPS.

6. Exceptions or qualifications:

This certificate is made with the knowledge that it will be relied upon by Canada.

This certificate shall remain in full force and effect and be binding upon the Department until a certificate repealing or replacing this certificate shall have been received by Canada and duly acknowledged in writing.

DATED at..this............day of................... , ...

----
signature of…………………., specify position

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 14 - ITS AND POLICY COMPLIANCE EVALUATION REPORT

The purpose of this report is to provide an analysis of the CCA's ITS and Policy Compliance Certificate and the CCA's CPS to confirm that the CCA satisfies the checklist security requirements. The Cross-Certification Team will conduct this analysis.

The document is to be organized in the following manner:

1. **Executive Summary**
   - Discrepancies
   - Key issues and rationale
   - Recommendations

2. **Description of security practices and safeguards**

3. **Compliance of the CCA's CP and CPS requirements**
   - Technical
   - Physical
   - Procedural
   - Personnel security

4. **Evaluation of security practices and safeguards**

5. **Analysis of the discrepancies associated with cross-certification**

6. **Key issues for consideration and rationale**

7. **Recommendations**
   - Proceed
   - Proceed with conditions

   DO NOT PROCEED

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 15 - CROSS-CERTIFICATION ARRANGEMENT

Document not finalized

NOTE: This document is Annex B of the Treasury Board Policy on Public Key Infrastructure Management in the Government of Canada. It may be amended from time to time by the signatories to the MOU

ANNEX 16 - GOVERNMENT OF CANADA PUBLIC KEY INFRASTRUCTURE INTERNAL CROSS-CERTIFICATION – MEMORANDUM OF UNDERSTANDING

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

INTERNAL CROSS-CERTIFICATION
MEMORANDUM OF UNDERSTANDING

among

TREASURY BOARD SECRETARIAT
("TBS")

and

DEPARTMENT OF NATIONAL DEFENCE,
COMMUNICATIONS SECURITY ESTABLISHMENT, in its capacity
as the Canadian Central Facility
("CCF")

and

DEPARTMENT OF NATIONAL DEFENCE,
COMMUNICATIONS SECURITY ESTABLISHMENT, in its capacity
as a "Department"

DEPARTMENT OF X

DEPARTMENT OF Y

(individually called a "Department", and
collectively called the "Departments")

1. Preamble

1.1 It is the policy of the Government of Canada to establish and manage the Government of Canada Public Key Infrastructure (GOC PKI) in order to provide for service delivery, public administration, and communications in a secure manner electronically.

1.2 The Departments wish to become members of the Policy Management Authority of the Government of Canada.

1.3 The Departments wish their Certification Authorities to be cross-certified with each other through the Canadian Central Facility (CCF), whereupon such cross-certified Certification Authorities become members of the Government of Canada Public Key Infrastructure.

1.4 The Departments, by entering into this Memorandum of Understanding (MOU), agree to the organizational structure of the GOC PKI described in this MOU, in the Government of Canada Certificate Policies, in government policies now existing or to be established, and in standards, guidelines and directions established by the Policy Management Authority.

2. Definitions

2.1 Words and expressions used in this Memorandum of Understanding mean: Canadian Central Facility (CCF) is the Government of Canada Public Key Infrastructure's central Certification Authority, and is operated by the Communications Security Establishment. Under Policy Management Authority direction, it serves as the Government of Canada's Level "0" Certification Authority. The Canadian Central Facility:

(a) provides the Policy Management Authority with technical assistance and support;
(b) signs and manages the cross-certificates of Departments' top-level Certification Authorities; and
(c) signs and manages the cross-certificates of top-level non-Government of Canada Certification Authorities with whom it has cross-certified.

Certification Authority (CA) is a person or organizational unit within a department that is responsible for:

(a) the operation of an authority trusted by one or more users to issue and manage public key certificates and certificate revocation lists; or
(b) the management of:
  (i) any arrangement under which a department contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and
  (ii) policies and procedures within the department for the management of public key certificates issued on its behalf.

A Certification Authority within a department remains, at all times, responsible and accountable for the management of public key certificates that it issues or has arranged to be issued on behalf of the department.

For purposes of this MOU, and except where otherwise specified, CA includes the CCF.

Certificate Policy (CP) is 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. It indicates whether or not the public key certificate is suitable for a particular application or purpose. A Certification Authority may adopt more than one Certificate Policy.

Certification Practice Statement (CPS) is a statement of the practices that a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and procedures of certificate life-cycle management, and is more detailed than the Certificate Policies supported by the Certification Authority.

Department means any Eligible Department which has become a party to this Memorandum of Understanding and for greater certainty, except where otherwise specified, includes CSE in its capacity as CCF.

Eligible Department includes all Departments and agencies listed in Schedule I, Parts I and II of the ***Public Service Staff Relations Act***, the Canadian Forces, and the Royal Canadian Mounted Police, and for greater certainty, except where otherwise specified, includes CSE in its capacity as CCF.

Employee is any person employed by a Department and, for greater certainty, does not include persons under contracts of service.

Government of Canada Public Key Infrastructure (GOC PKI*)* is a public key infrastructure for use by Departments, which operates in accordance with standards, guidelines, and directions of the Policy Management Authority.

Policy Management Authority (PMA) is responsible for the oversight and policy management of the Government of Canada Public Key Infrastructure. It makes recommendations to the Secretary of the Treasury Board with respect to cross-certification, and provides a horizontal management structure and policy framework for the management and operation of the Government of Canada Public Key Infrastructure. Its permanent membership includes a representative of the CCF, and of each Department having at least one (1) CA which is a member of the GOC PKI. Representatives are appointed by the Secretary of the Treasury Board on the recommendation of the deputy head of each Department. Each such Department will be entitled to one (1) vote on the PMA, and the representative of the CCF has one (1) vote in that capacity. The chairperson of the PMA is appointed by the Secretary of the Treasury Board. In the interim until April 1, 2001, the PMA will consist of such Departmental representatives and others as the Secretary of the Treasury Board may appoint, (including any representatives of the permanent PMA appointed under section 4.2 hereof), with the Departments so represented and others so appointed having one (1) vote each, and the chairperson and CCF having one (1) vote each.

Repository is a system for storing and accessing certificates or other information relevant to certificates.

2.2 Any words or expressions not defined in this Memorandum of Understanding have the meaning assigned to them in the Government of Canada Certificate Policies, as amended from time to time, located on the Treasury Board Secretariat Public Key Infrastructure web site at www.cio-dpi.gc.ca (hereinafter called “GOC CP”). In the event of an inconsistency or ambiguity, the definitions or meaning in this Memorandum of Understanding shall prevail, unless otherwise specified.

3. Parties

3.1 The parties to this Memorandum of Understanding (“MOU”) agree that:

(a) from time to time, this MOU will be signed by additional Eligible Departments;

(b) any additional member Departments are subject to this MOU as if they were original parties to this MOU, and all other Departments are subject to this MOU with regard to the additional Departments as each additional Department signs this MOU, as if the additional Departments were original parties to this MOU; and

(c) from time to time, this MOU may be terminated with regard to one or more Departments in accordance with section 8.

4. Effective Date of this MOU

4.1 This MOU becomes effective with respect to a Department's Certification Authority on the day that the Canadian Central Facility issues a cross-certificate to that Certification Authority and publishes it in an appropriate Repository.

4.2 Each Department shall, upon the issuance and publication of the said cross-certificate to at least one Certification Authority of that Department, recommend for membership in the PMA, and for appointment as such by the Secretary of the Treasury Board, one senior official per Department, and each such Department will be entitled to one vote.

4.3 This MOU remains in effect for so long as there are at least two (2) Departments (excluding the CCF) having CAs that are cross-certified with the Canadian Central Facility.

5. Membership in the GOC PKI

5.1 Membership in the GOC PKI is open only to Eligible Departments.

5.2 Each Department agrees to be bound by and to comply with the standards, guidelines, practices and directions of the PMA.

5.3 Each Department agrees to ensure that its CAs which are members of the GOC PKI (“member CAs”) comply with the provisions of any applicable policy, statute or regulation of Canada in force from time to time. In particular, each Department agrees to:

(a) implement and maintain appropriate security at least to the standard set out in its CPs;
(b) comply with the provisions of its CPs;
(c) issue public key certificates only to those subscribers/relying parties, other than Employees, who have signed an agreement, and only to those Employees who have been apprised of the Department's policy on the use of public key certificates;
(d) cross-certify with other Departments or with anyone other than a Department only through the CCF acting on the direction of the PMA;
(e) remain responsible and accountable for the acts and omissions of its CAs notwithstanding that any of the CA services are provided by another Department or by an external service provider; and
(f) provide access for any compliance inspections as are required to be made pursuant to the GOC PKI.

5.4.1 Where a Department has established a member CA and intends to cross-certify with another of its CAs that is not a member of the GOC PKI (“non-member CA”), then such Department shall inform the PMA. Where the PMA is of the opinion that this cross-certification may adversely affect the GOC PKI, then the PMA may take appropriate action, including downgrading or revoking the cross-certificate it issued to the member CA, and publishing notice of same in the appropriate Authority Revocation List (“ARL”).

5.4.2 Any such downgrade or revocation shall be subject to a vote of the PMA in the same manner as for termination under section 8.1, and the provisions of sections 8.1 and 8.3 shall also apply to the extent that revocation results in the termination of a CA or the Department, as the case may be, and in the case of a downgrade to the extent appropriate for the proper administration of the GOC PKI.

5.5 The CCF agrees:

(a) to adopt the Government of Canada Certificate Policies located at www.cio-dpi.gc.ca as its CP; and

(b) to issue cross-certificates to CAs, or to downgrade or revoke cross-certificates of CAs, on the direction of the PMA.

5.6 The Departments acknowledge that certain information about their Employees, and subscribers/relying parties other than Employees, may be contained in certificates and in public Repositories, agree that they will comply with the provisions of the ***Privacy Act*** and other applicable privacy law, the ***Access to Information Act***, and the Treasury Board policies on Access to Information and Privacy with respect thereto, and will secure the agreement of their agents, contractors, or subcontractors to so comply.

6. Repository

Each Department shall:

(a) have a Repository associated with its CA;

(b) ensure that the Repository associated with its CA is maintained in such a manner that any information it contains is current, accurate, and conforms with the requirements of the CA's Certificate Policy;

(c) register its Repository with the Government of Canada registrar for Repository service providers;

(d) ensure that its public key certificates and Certificate Revocation Lists ("CRLs") are published in its Repository; and

(e) ensure that its Repository conforms to applicable Government of Canada Repository standards and is interoperable with other repositories associated with Certification Authorities who are parties to this MOU.

7. Financial Responsibility

7.1 Where Her Majesty in right of Canada is held liable for the payment of money to any person outside of the Government of Canada pursuant to a final judgement, award, or settlement arising out of an act or omission of a Department's CA, then such payment shall be made by Her Majesty the Queen in right of Canada and, with respect to a judgement, shall be made in accordance with section 30 of the *Crown Liability and Proceedings Act*.

7.2 In the event that the liability referred to in section 7.1 is incurred as a result of the act or omission of the CAs of more than one (1) Department, including the CCF, then financial responsibility shall be allocated amongst them in proportion to the degree of fault, determined as follows:

(a) by agreement of the Departments. If the Departments fail to agree within 60 calendar days of the date of the judgement, award or settlement, then

(b) in accordance with the procedure for dispute resolution set out in section 9.

7.3 In the event that a Department makes a payment to any person outside of the Government of Canada who was not entitled to it, in reliance on an act or omission of the

CA of another Department or Departments, and such payment is not recovered despite reasonable efforts within a year, then the Department(s), including the CCF, whose act or omission resulted in the loss shall reimburse the Department which made the payment. Financial responsibility shall be allocated amongst the Departments responsible for the loss in proportion to the degree of fault, determined as follows:

(a) by agreement of the Departments. If the Departments fail to agree within 60 calendar days of the expiration of the year, then
(b) in accordance with the procedure for dispute resolution set out in section 9.

7.4 In the event that the liability under section 7.2, or the payment under section 7.3, cannot reasonably be attributed to the act or omission of a CA or CAs, then financial responsibility shall be apportioned amongst the Departments, excluding the CCF, whose CAs were involved in the event giving rise to the liability or payment. Any dispute as to the application or interpretation of this section shall be referred to the dispute resolution process set out in section 9.

7.5 Notwithstanding anything in this MOU, if a Department establishes limits on liability higher than those set out in the GOC CP then, subject to any other written arrangement it may make, it is solely accountable for the difference between the liability limit in the GOC CP and its own higher liability limit. Any dispute as to the application or interpretation of this section shall be referred to the dispute resolution process set out in section 9.

7.6 No Department shall be responsible for a payment or reimbursement pursuant to any settlement unless it has consented to the settlement.

8. Termination; Withdrawal

8.1 Notwithstanding anything contained in the Department's CP, where a Department or its CA(s) is in default of any of its responsibilities under this MOU, the President of the Treasury Board of Canada may, on the recommendation of the Secretary acting on the advice of the PMA made by a three/quarters vote of all members present at a meeting of the PMA held for that purpose excluding the vote of the member of the said Department, give notice to the Department terminating the membership of the Department or of its CA, as the case may be, in the GOC PKI, either immediately, or at the expiration of a cure period specified in the notice if the Department or CA has not cured the default to the satisfaction of the President within that cure period. If the membership of the Department is so terminated, then the appointment of that Department's member to the permanent PMA is also terminated without additional notice.

8.2 A Department wishing to terminate the operation of one or more of its CAs must, by at least 30 calendar days' prior notice to the PMA:

(a) withdraw a specific CA or CAs from membership in the GOC PKI; and
(b) in the case of termination of the operation of all its CAs, then withdraw from membership in the PMA.

8.3 In the event of termination or withdrawal under sections 8.1 or 8.2 of the Department or of one or more of its CAs, then, as soon as possible prior to the effective date of such termination or withdrawal, if not already done:

(a) the CCF shall revoke the cross-certificate(s) of the Department or the CA, and publish notice of the revocation in the appropriate Authority Revocation List;

(b) the CA will revoke all certificates which it has issued, provide appropriate notice of such revocation to subscribers, and publish notice of the revocation in the appropriate Certificate Revocation List; and

(c) transfer or cause to be transferred to the PMA, or as the PMA may direct, for appropriate action, all its Repository records, private confidentiality keys retained by it, and other records, archival material, audit logs, CPS, or any other information or thing necessary for the continued and uninterrupted provision of services and for reissuance of certificates, all as determined in the discretion of the PMA.

8.4 Notwithstanding anything contained in this MOU, the Communications Security Establishment will not terminate or withdraw from the GOC PKI as manager and operator of the CCF unless the PMA has first given its approval and appropriate arrangements have been made for the transfer of the CCF responsibilities, functions, records, or any other information or thing necessary for the continued and uninterrupted provision of CCF services and for re-issuance of cross-certificates, if necessary, all as determined in the discretion of, and in a manner satisfactory to, the PMA.

8.5 Unless otherwise provided herein, any other provision for termination or withdrawal of a Department or a CA from the GOC PKI contained in that Department's CP also applies. In the event of any conflict or inconsistency between this section 8 and the Department's CP, then, unless otherwise provided herein, the provisions of this section 8 shall prevail.

9. Dispute Resolution

9.1 The parties to a dispute hereby undertake to use their best efforts to resolve any dispute in an amicable and expeditious manner, first by negotiation and, failing resolution, then through an independent mediator, as follows:

(a) Any party may, by notice in writing or by digitally signed electronic message, commence negotiations.

(b) If the dispute is not resolved within 90 calendar days of the notice to commence negotiations, then either party may, by notice in writing or by digitally signed electronic message, submit the dispute to mediation.

(c) A single independent mediator, not being an employee or contractor of the parties, shall be appointed by the parties and, failing such appointment within 30 calendar days of the submission to mediation, the mediator shall, upon application by one or both of the parties, be appointed by the PMA within 30 calendar days after the expiration of the previous 30-day period.

(d) The costs of negotiation, or the mediation, as applicable, including the fees of the mediator, the mediator’s travel and accommodation expenses, and the costs of room rental and support services for the negotiation or mediation proceedings, shall be shared equally by the parties.

(e) Each party shall bear its own costs of legal representation, travel and accommodation for the negotiation or mediation, as applicable.

9.2 Any dispute which has not been resolved in the manner described within 90 calendar days of the appointment of the mediator as set out in 9.1 above shall then, but cannot before the lapse of the time periods set out for negotiation and mediation in 9.1 above, be referred to the PMA. The PMA shall, by a 51% vote of members present at a meeting held for the purpose, excluding the votes of members of the parties to the dispute, within 30 calendar days after the expiration of the previous 90-day period, appoint an expert in the subject-matter of the dispute who shall decide the dispute. The expert shall not be an employee or contractor of any of the parties to the dispute. The decision of the expert is binding on the parties and enforceable as an obligation of the parties under this MOU. In making its decision, the expert shall follow the rules of procedure established from time to time by the PMA.

10. Notice

10.1 Where this MOU calls for notice or notification, unless specified otherwise, such notice may be delivered by hand, by mail, by courier, by facsimile, or by digitally signed electronic mail. A notice shall be deemed to have been received on the fifth business day after mailing if sent by regular mail, on the date of delivery if sent by courier, and on the first business day after the date of transmission if sent by facsimile or electronic mail.

10.2 Delivery of notice to a Department in care of its representative on the PMA shall constitute notice to that Department for purposes of this MOU.

10.3 Delivery of notice to TBS in care of the chairperson of the PMA shall constitute notice to the TBS for purposes of this MOU. Notice to the chairperson of the PMA is to:

PMA Secretariat
Treasury Board Secretariat
275 Slater Street, 6th fl.
Ottawa, Ontario
K1A 0R5.

10.4 Delivery of notice to the CCF in care of its representative on the PMA shall constitute notice to the CCF for purposes of this MOU. Notice to the CCF is to:

Director, T
Communications Security Establishment.
P.O. Box 9703, Terminal
Ottawa, Ontario.
K1G 3Z4

11. General

11.1 This MOU may be amended in writing signed by all the parties. Amendments made from time to time to the GOC CP do not constitute such amendments to this MOU.

11.2 This MOU or any amendment thereto may be signed in counterpart.

11.3 The provisions of this MOU with respect to financial responsibility, dispute resolution, and any other responsibilities or obligations not resolved or completed by a Department upon such revocation, termination or withdrawal, shall survive the revocation of a cross-certificate under section 5, or the termination or withdrawal of a Department or its CA(s) under section 8.

______________________________ Secretary of the Treasury Board for the Treasury Board Secretariat	______________________________ Chief, Communications Security Establishment
______________________ Date	______________________ Date

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 17 - NEGOTIATION REPORT

The purpose of this report is to document the differences between the model and the negotiated arrangement. The document is to be prepared by the Cross-Certification Team.

The document is to be organized in the following manner:

1. **Executive Summary**
   Status of negotiations
   Points of disagreement
   Key issues and rationale
   Recommendations

2. **Description of the status of the negotiations**

3. **Description of the points disagreement**
   Clauses in which changes have been made
   Description of deviation from model arrangement and reasons

4. **Analysis of impact and possible consequences of changes and deviations**

5. **Key issues for consideration and rationale**

6. **Recommendations**
   Proceed
   Proceed with conditions
   Do not proceed

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 18 - CONSOLIDATED EVALUATION REPORT

The purpose of this report is to consolidate relevant information from CP Mapping Report, the Testbed Trial Report and the System Survey, the ITS and Policy Compliance Evaluation Report, and the Negotiation Report to enable the PMA to make a decision on cross-certification. The report is to be prepared by the Cross-Certification Team.

The document is to be organized in the following manner:

1. Executive Summary

- Points of discrepancies and disagreements
- Key issues and rationale
- Recommendations

2. Summary of Issues from the four major Reports

- CP Mapping Report
  - Discrepancies
  - Analysis of impacts and risk
- Testbed Trial Report and the System Survey
  - Discrepancies
  - Analysis of impacts and risk
- ITS and Policy Compliance Evaluation Report
  - Evaluation of security practices and safeguards
  - Discrepancies
  - Analysis of impacts and risk
- Negotiation Report.
  - Points of disagreement
  - Clauses in which changes have been made
  - Description of deviation from model arrangement and reasons
  - Analysis of impact and possible consequences of deviations or changes

3. Analysis of possible implications associated with cross-certification

4. Key issues for consideration and rationale

5. Recommendations

- Cross-certify without conditions
- Cross-certify with conditions
- Do not cross-certify

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ARTICLE 19 - COMPLIANCE REVIEW REPORT

The purpose of this report is to detail the results of a Compliance Review of an Affiliated CA. A Compliance Review may be initiated for cause by the PMA resulting from information received in a Compliance Certificate, issues that may arise from Problem Reports or Change Management Report, or changes to technology, business or legal circumstances.

The document is to be organized in the following manner:

1. **Executive Summary**
   Affiliated CA
   Discrepancies or areas of concern
   Key issues and rationale
   Recommendations

2. **Cause for Compliance Review**

3. **Results of the Compliance Review**
   Discrepancies and areas of concern

4. **Description of Issues, if any**
   Policy
   Administrative
   Technological
   Legal
   Financial

5. **Corrective action taken or recommended**

6. **Analysis of possible implications associated with the continuation of the existing cross-certification arrangement**

7. **Key issues for consideration and rationale**

8. **Recommendations**
   Continue Affiliated CA's cross-certification at its current level of assurance with the CCF
   Downgrade the assurance level of the cross-certificate with the CCF
   Terminate the Affiliated CA's cross-certification certificate with the CCF.

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 20 - PROBLEM RESOLUTION REPORT

The purpose of this report is to identify disputed problems that may be encountered by any of the parties involved in a cross-certification agreement and to provides information to enable a problem resolution. A Problem Report may be initiated by any party to the cross-certification agreement and sent to the responsible PMA PKI Desk Officer for action. The Desk Officer will authenticate the information, co-ordinate responses, attempt to resolve outstanding issues and report on resolution results. The report is organised into three parts. Relevant supporting documentation should be attached.

The document is to be organized in the following manner:

Part I: Problem Report – Reporting Party

(This part states the problem from the Reporting Party's point of view.)

1. Affiliated CA
2, Problem description
3. Key issues and areas of dispute
4. Proposed solution to resolve the problem

Part II: Problem Review – Desk Officer

(This part states other relevant information, precedence and recommends solutions)

5. Problem authentication
6. Alternate points of view
7. Identify any precedents
8. Steps taken to resolve the issues
9. Description of key issues, if any
10. Analysis of possible implications associated with the cross-certification arrangement
11. Key issues for consideration and rationale
12. Recommendations to resolve dispute, if required

Part III: Problem Resolution – Desk Officer

(This part documents the outcome.)

13. Resolution decision and rationale for decisions
14. Consequence or effect of issue on compliance
15. Conditions

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 21 - CHANGE MANAGEMENT REPORT

The purpose of the report is to evaluate proposed changes to ensure that the integrity of the cross certification arrangement and participating Affiliated CA's PKI is maintained. The report identifies proposed changes to a CA and the potential effect on performance, risk, existing policy and standards. The report may be initiated by any party to the cross certification arrangement and sent to the responsible PMA PKI Desk Officer. The Desk Officer authenticates the information, co-ordinates all responses, provides an analysis of the changes, provides recommendations and reports on the results. The report is organised into three parts. Relevant supporting documentation should be attached.

The document is to be organized in the following manner:

Part I: Proposed Change – Reporting Party
(This part states the proposed change from the reporting party's perspective)

1. Affiliated CA
Description of the proposed change(s)
Reason for proposed change

2. Discussion of policy, technical and legal issues
Anticipated effect on system performance
Anticipated effect on cross-certification arrangement and compliance issues
Adjustments or changes to cross-certification arrangement

3. Recommended change, rationale and statement of risk

Part II: Analysis of proposed change - Desk Officer
(This part states other relevant information, precedents, and an analysis of the proposed change and recommendations)

4. Authentication of the proposed change

5. Analysis of proposed change
Potential effects on existing arrangement or performance
Divergences from cross-certification arrangement

6. Key issues associated with the proposed change and rationale

7. Recommendation to the PMA
Proceed
Proceed with conditions
Do not proceed

Part III: Change Proposal Resolution – Desk Officer
(This part documents decisions and out comes of the change proposal resolution process)

8. PMA decision, conditions and rationale

GOVERNMENT OF CANADA
PUBLIC KEY INFRASTRUCTURE

ANNEX 22 - RENEWAL/TERMINATION REPORT

The purpose of this report is to summarise all relevant issues and information from documentation to support a PMA decision to renew or terminate an existing cross-certification arrangement. This report will be used to renew an existing arrangement, to terminate an arrangement by an external CA, to withdraw from an arrangement by a GOC PKI member, or to terminate an arrangement by the PMA.

Part I: Request for Renewal or termination – Desk Officer or any party to the arrangement

(Initiated by any party, or automatically by the desk officer 180 days in advance of the expiration of a CA's cross-certification arrangement.)

1. Reasons for renewal or termination

2. Desired date

<u>Part II: Analysis of renewal/termination request - Desk Officer</u>

(Desk officer staffs the request for a decision by the PMA.)

3. Description of Affiliated CA

4. Description of issues, if any

5. Analysis of implications of renewal or termination, if required

6. Key issues for consideration and rationale

7. Recommendations

Renew
Renew with conditions
Terminate or withdraw from arrangement

<u>Part III: Decisions – Desk Officer</u>

(Decisions and out comes of the decision to renew or terminate the arrangement)

8. PMA decision and conditions

9. Date of withdrawal/termination