Air Canada Public Key Infrastructure

Certificate Policy

Validation and signature of the PMA CHAIR:

Shaun Harrison

Author: Carillon Information Security Inc.

Date: June 18, 2024
Version: 1.5
Classification: **PUBLIC**
Status: FINAL

Version Information

1.0	June 21, 2017	Carillon Information Security Inc.	Initial document
1.1	December 21, 2017	Carillon Information Security Inc.	CR-01 – Minor typographical and formatting adjustments throughout the document Device Email Signature - Modify content in section 10.7. CR-02 – Modifications for Certipath Certificate Policy (v.3.32) compliance Add or modify content in the following sections: 1.1.4; 1.3; 1.3.1; 1.3.6.2; 1.6.2; 3.2.3.1; 3.2.3.3; 3.2.3.4; 4.3.1; 4.9.13; 4.9.14; 4.9.15; 4.9.16; 4.12.1; 5.1.1; 5.1.2.1; 5.2.1; 5.2.3; 5.2.4; 5.3.1; 5.3.2; 5.3.3; 5.3.7; 5.3.8; 5.4; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.6; 5.5.1; 5.5.2; 5.5.3; 5.7; 5.7.1; 5.7.3; 5.8; 6.1; 6.1.1; 6.1.6; 6.1.7; 6.2.6; 6.2.8; 6.2.9; 6.2.10; 6.3.3; 6.4.1; 6.5.1; 6.6.1; 6.6.2; 6.7; 6.8; 8.1; 8.3; 10.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5; 10.1.6; 10.1.7; 10.1.8; 10.2.1; 10.2.2; 10.2.3; 10.2.4; 10.2.5; 10.2.6; 10.2.7; 10.2.8; 10.2.9; 10.2.10; 10.2.11; 10.2.12; 10.2.13; 10.2.14; 10.3.1; 10.5; 10.6; 10.7. CR-03 – Addition of examples of Prohibited Certificate uses Modify content in section 1.4.2.
1.2	February 17, 2022	Carillon Information Security Inc.	CR-01 – Modify formatting of cover page Modify the following sections: 5.6, 6.1.1, 10.1.7, 10.7 to remove incorrect terminology Throughout the document – Minor typographical and formatting adjustments CR-02 – Certificate Policy review and update Add or modify content in the following sections: 1.5.2; 1.6.2; 2.2.1; 2.4; 4.8; 6.2.4.2; 9.6.2; 10.2.8; 10.2.10; 10.2.11; 10.7 Remove content in the following sections: 1.3.6.2; 10.1.3; 10.1.4; 10.2.1 CR-03 – Alteration to the Certificate Acceptance

			requirement for Basic LoA Device Certificates Modify content in section 4.4.1 CR-04 - Review and modifications to the Private Key and Certificate Validity Periods Modify content in the following sections: 5.6; 10.1.7; 10.2.7; 10.2.8; 10.2.9; 10.2.10; 10.2.11; 10.2.12
1.3	April 26, 2022	Carillon Information Security Inc.	CR-01 – Minor adjustments (Version number, Date, Table of contents) Updated RFC reference Modify content in the following sections: 4.9.10; 7.3; 10.4 Modify suspension requirement to conform to operational practice Modify content in the following section: 4.9.13 CR-02 – Addition of E-EGS Aircraft Identity and Issuing certificate in the table Add content in the following section: 5.6 CR-03 – Changes to add new level of assurance and certificate type related to Boeing requirements Add/modify content in the following sections: 1; 1.2; 1.3.6; 3.3.1; 4.9.5; 5.6; 6.1.1; 7.1.6; 10.2.12; 10.7
1.4	February 16, 2023	Carillon Information Security Inc.	CR-01 – Minor adjustments (Version number, Date, Table of contents) CR-02 – Add information related to vulnerability assessments Modify content in the following section: 5.4.8 CR-03 – Modify the requirements for backing up device subscriber private signature keys Modify content in the following section: 6.2.4.2 CR-04 – Addition of new subsection 8.7 Add content in the following section: 8 CR-05 – Modification of the sections regarding Confidentiality and Privacy for easier mapping to RFC 3647 Add and modify content in the following sections: 9.3; 9.4

1.5	June 18, 2024	Carillon Information Security Inc.	CR-06 - Addition of the optional Microsoft Directory Service extension in subscriber ID certificates Add content in the following section: 10.2.1 CR-01 – Minor adjustments (Version number, Date, Table of contents) Minor typographical and formatting adjustments throughout the document CR-02 – Adjustments to reflect current operational practice - Modify the OU in a subject name - Change audit frequency to every 2 years - Correct certificate profile Modify content in the following sections: 7.1.4; 8.1; 10.1.5 CR-03 – Adjustment to reflect current PMA Chair Modify content in the following section: 1.5.2

Document References

Document references found throughout this Certificate Policy are listed in the Air Canada PKI Referenced Documents Table.

Table of Contents

1 Introduction

This Certificate Policy defines several policies applicable to the use of digital certificates for authentication, integrity (through digital signatures) and encryption in order to provide digital Certificates to End-Entities.

The policies represent the following Assurance Levels for Public Key Certificates:

- basic-software-256
- basic-hardware-256
- medium-software-256
- medium-hardware-256
- medium-device-software-256
- medium-device-hardware-256
- BEGSS
- BEGSS-hardware
- E-EGS
- E-EGS-hardware

The word "assurance" used in this CP means how well a Relying Party (RP) can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was used to produce the Certificate and (if appropriate) deliver the Private Key to the Subscriber performs its task.

The Air Canada PKI will be required to comply with the Certification Policy of other PKI domains CAs or Bridge CAs to which it is cross-certified through the use of policy mapping or direct policy assertion.

This policy covers the Air Canada Root CAs and the certified subordinated Air Canada Subordinate CAs. The Air Canada Principal CAs (PCAs) may cross certify with other PKI domains in order to allow interoperation with other Enterprises required for the business of Air Canada, its Business Units, affiliated companies, and customers.

Any use of or reference to this CP outside the purview of the Air Canada PKI is completely at the using party's risk. Only the Air Canada Root CAs and Subordinate CAs of those roots shall assert the OIDs listed in section 1.2 of this document in any Certificates issued by the Air Canada PKI, except in the policyMappings extension of Certificates issued by the CAs cross-certified with an Air Canada PCA for the establishment of equivalency between Air Canada and external PKI domains Assurance Levels.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

Certificates issued by Air Canada contain one or more registered Certificate Policy object identifiers (OIDs) which may be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. Each OID corresponds to a specific level of assurance established by this CP. This CP shall be available to Relying Parties in accordance with the publication rules set forth in section 2.

Cross-certificates issued by an Air Canada PCA shall, in the policyMappings extension and in whatever other fashion is determined by the Air Canada Policy Management Authority (Air Canada PMA, cf. section 1.3.1) to be necessary for interoperability, reflect what mappings exist between this CP and the cross certified PKI domains' CPs.

1.1.2 Relationship between this CP and an Air Canada PKI CPS

This CP states what assurance can be placed in a Certificate issued under this policy. The Air Canada Certification Practice Statements (Air Canada CPSes) state how the Air Canada CAs establish that assurance.

1.1.3 Relationship between this CP, the other PKI domains' CPs

The levels of assurance of the Certificates issued under this CP are mapped by the Air Canada Policy Management Authority (Air Canada PMA) to the levels of assurance of the Certificates issued by other PKI domains which cross certify with an Air Canada PCA. The policy mappings information is placed into the Certificates issued by an Air Canada PCA, or otherwise published or used by the Air Canada PKI Operational Authority (described in section 1.3.1.2) so as to facilitate interoperability.

1.1.4 Scope

Figure 1 illustrates the scope of this CP.

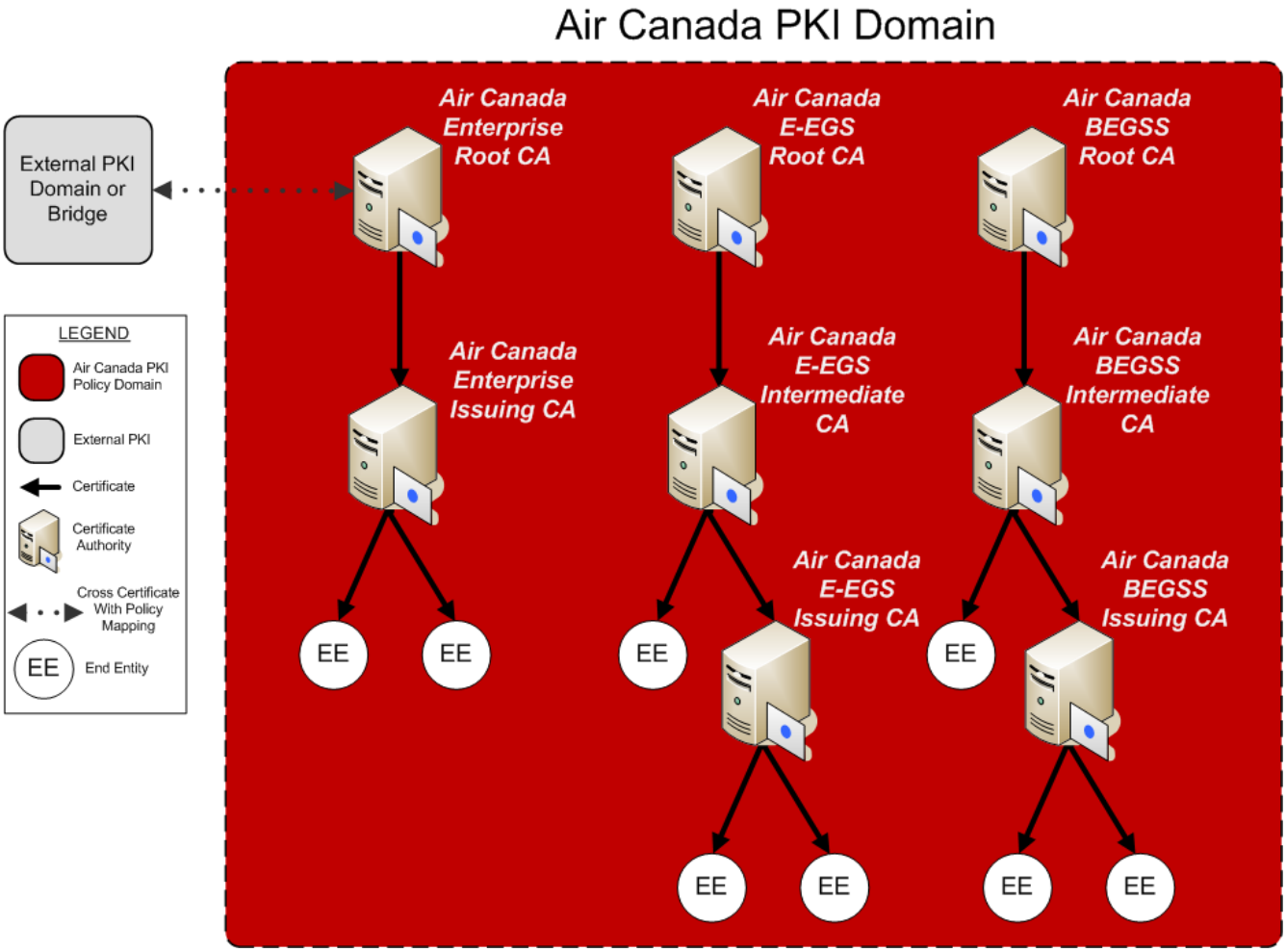

Figure 1 – Scope and Domain of Air Canada CAs

This CP imposes requirements on all the Air Canada CAs and other PKI domains involved in issuing Certificates. These include the following:

- the Air Canada Enterprise Root Certification Authority (Air Canada Enterprise Root CA);
- the Air Canada E-EGS Root Certification Authority (Air Canada E-EGS Root CA);
- the Air Canada BEGSS Root Certificate Authority (Air Canada BEGSS Root CA);
- all Air Canada Certification Authorities directly subordinated to an Air Canada Root CA (Air Canada Subordinate CAs)[1];
- cross-certified PKI domains' CAs.

The Air Canada Root CAs shall issue CA Certificates only to Air Canada Subordinate CAs

[1] For BEGSS and E-EGS, only the Intermediate CAs are in scope, not the Issuing CAs.

approved by the Air Canada PMA.

The Air Canada Root CAs may also issue Certificates to individuals who operate the Air Canada Root CAs or devices necessary for the operation of the Air Canada Root CAs.

The Air Canada PCAs shall issue CA Certificates only to other PKI domains' CAs approved for cross certification by the Air Canada PMA.

The Air Canada Enterprise Root Certification Authority is the only PCA for the Air Canada PKI.

Air Canada Subordinate CAs may issue Certificates to individuals, roles, devices (including ground systems, aircraft, and aircraft avionics), at any Assurance Level consistent with the Assurance Levels and type delegated to that Subordinate CA by its issuing CA. For BEGSS and E-EGS, Air Canada Subordinate CAs may also issue Certificates to CAs, at any Assurance Level consistent with the Assurance Levels and type delegated to that Subordinate CA by its issuing CA; these Subordinate CAs are also known as Intermediate CAs.

The Air Canada Root CAs and Air Canada Subordinate CAs exist to facilitate trusted communications within the Air Canada Domain and with Air Canada partners, customers, and regulatory authorities either directly or through cross-certification with other PKI domains.

Within this document, the term CA, when used without qualifier, shall refer to any certification authority subject to the requirements of this Certificate Policy, including the Air Canada Root CAs and Air Canada Subordinate CAs.

The term Air Canada Subordinate CAs shall refer to any Subordinate CA within the Air Canada PKI.

Requirements that apply to a specific CA type will be denoted by specifying the CA type, e.g., Air Canada Root CAs, Air Canada Subordinate CAs, other PKI domains' CAs, etc.

The scope of this CP in terms of Subscriber (i.e., End-Entity) Certificate types is limited to those listed in section 10.

1.2 Document Name and Identification

This document is called the Air Canada PKI Certificate Policy (CP).

There are several levels of assurance in this Certificate Policy, which are defined in subsequent sections.

Each Assurance Level is uniquely represented by an "object identifier" (OID), which is asserted in each Certificate issued by the Air Canada Subordinate CAs that complies with the policy stipulations under this CP.

The OIDs are registered under the Air Canada arc as follows:

Certificate Name	OID
id-basicSoftware-256	::= {1.3.6.1.4.1.49507.1.1.9}
id-basicHardware-256	::= {1.3.6.1.4.1.49507.1.1.10}
id-mediumSoftware-256	::= {1.3.6.1.4.1.49507.1.1.11}

id-mediumHardware-256	::= {1.3.6.1.4.1.49507.1.1.12}
id-mediumDeviceSoftware-256	::= {1.3.6.1.4.1.49507.1.1.13}
id-mediumDeviceHardware-256	::= {1.3.6.1.4.1.49507.1.1.14}
id-begss	::= {1.3.6.1.4.1.49507.1.2.1}
id-begssHardware	::= {1.3.6.1.4.1.49507.1.2.2}
id-eegs	::= {1.3.6.1.4.1.49507.1.3.1}
id-eegsHardware	::= {1.3.6.1.4.1.49507.1.3.2}

The Air Canada PMA shall not request any "pass-through" policy OIDs to be asserted in any cross-certificates issued to them by an external PKI domain.

Unless otherwise noted, a requirement stated in this CP applies to all Assurance Levels.

Unless otherwise noted, a requirement stated in this CP for the id-mediumHardware-256 Assurance Level applies to the id-mediumDeviceHardware-256 Assurance Level, id-begssHardware and id-eegsHardware.

Unless otherwise noted, a requirement stated in this CP for the id-mediumSoftware-256 Assurance Level applies to the id-mediumDeviceSoftware-256, id-begss and id-eegs Assurance Levels.

CAs must use SHA-256 for generation of PKI objects such as Certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses.

Figure 2 illustrates the ordered hierarchy of these policies:

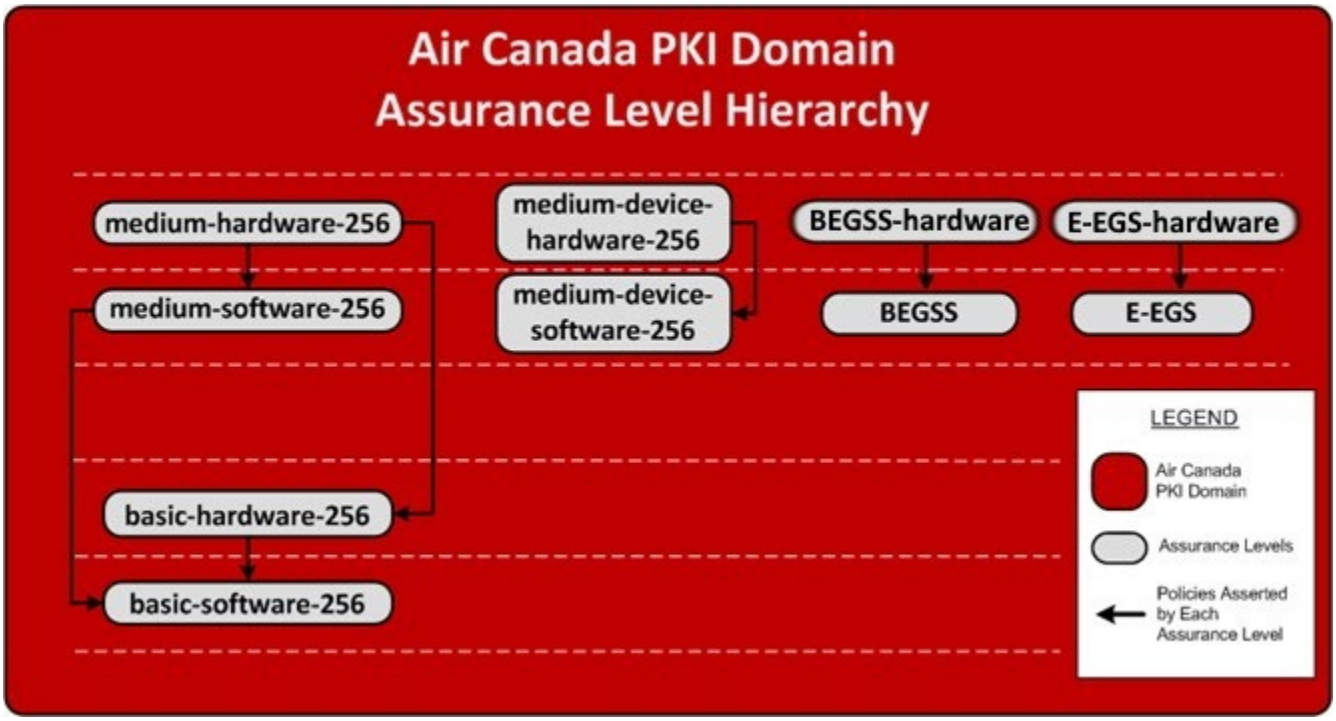

Figure 2 – Assurance Level Hierarchy and Policy Assertion Direction

1.3 PKI PARTICIPANTS

This section contains a description of the roles relevant to the administration and operation of the Air Canada CAs. The PKI components identified in Sections 1.3.1.4 through 1.3.2 and their sub-components comprise the security-relevant components of the PKI and must adhere to the security, audit and archive requirements of Sections 5 and 6.

1.3.1 Air Canada PKI Authorities

1.3.1.1 Air Canada Policy Management Authority (Air Canada PMA)

The Air Canada PMA is responsible for:

- Commissioning, drafting and approving the Air Canada PKI CP (this document);
- Commissioning compliance analysis, acting on recommendations resulting from analysis, and approving the Air Canada PKI CPSes;
- Ensuring continued conformance of the Air Canada PKI CPSes with applicable requirements as a condition for continued securing of the Assurance Levels as stipulated in this CP;
- Accepting and approving applications from entities desiring to cross-certify with an Air Canada PCA;
- Managing the interoperation with other PKI domains' CAs;
- Ensuring continued conformance of the Air Canada PKI and other domains' PKI with applicable requirements as a condition for allowing continued interoperability with cross-certified CAs.

Air Canada shall enter a contractual relationship through a Memorandum of Agreement (MOA) with the PMAs of other PKI domains setting forth the respective responsibilities and obligations of both parties, and the mappings between the Certificate levels of assurance contained in this CP and those in the respective CP of the other PKI domains' CA subject to cross-certification. The term "MOA" as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

A complete description of Air Canada PMA roles and responsibilities is provided in the Air Canada PKI Policy Management Authority Charter [PMA Charter and Bylaws].

1.3.1.2 Air Canada PKI Operational Authority (OA)

The Air Canada PKI Operational Authority consists of the organisations that are responsible for the operation of the Air Canada CAs, including issuing Certificates when directed by the Air Canada PMA or any authorised Air Canada Registration Authority (RA) operating under this CP, posting those Certificates and Certificate Revocation Lists (CRLs) into the repositories of the Air Canada PKI, and ensuring the continued availability of these repositories to all users in accordance with section 2 of this document.

1.3.1.3 Air Canada PKI Operational Authority Administrator

The Administrator is the individual within the Operational Authority who has principal responsibility for overseeing the proper operation of the Air Canada PKI infrastructure components, and who appoints individuals to the positions of Operational Authority Officers.

The Administrator is selected by and reports to the Air Canada PMA.

The Administrator approves the issuance of Certificates to the other trusted roles operating the Air Canada PKI CAs.

1.3.1.4 Air Canada Principal Certification Authority (PCA)

A Principal CA is a CA within a PKI that has been designated by the PMA to interoperate directly with an external domain CA (e.g., through the exchange of cross-certificates).

As operated by the Operational Authority, an Air Canada PCA is responsible for all aspects of the issuance and management of a Cross-Certificate issued to an external domain CA, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Cross-Certificate manufacturing process,
- The publication of Cross-Certificates,
- The revocation of Cross-Certificates,
- Ensuring that all aspects of the services, operations and infrastructure related to Cross-Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.5 Air Canada Root CAs

An Air Canada Root CA is a trust anchor for Relying Parties trying to establish the validity of a Certificate issued by an Air Canada Subordinate CA, whose chain of trust can be traced back to that specific Root CA.

An Air Canada Root CA issues and revokes Certificates to Air Canada Subordinate CAs upon authorisation by the Air Canada PMA. As operated by the Operational Authority, an Air Canada Root CA is responsible for all aspects of the issuance and management of those Subordinate CA Certificates, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Certificate manufacturing process,
- The publication of Certificates,
- The revocation of Certificates, and
- Ensuring that all aspects of the services, operations and infrastructure related to Subordinate CA Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

An Air Canada Root CA may function as a PCA.

1.3.1.6 Air Canada Subordinate CAs

The Air Canada Subordinate CAs are all the Signing CAs and Intermediate CAs subordinate to an Air Canada Root CA as defined below.

An Intermediate CA is a CA which is not a Root CA and issues Certificates to other CAs within the Air Canada PKI. Intermediate CAs may or may not issue Certificates to End-Entities.

A Signing CA is a CA whose primary function is to issue Certificates to End-Entities. A Signing CA does not issue Certificates to other CAs.

As operated by the Operational Authority, an Air Canada Signing CA is responsible for all aspects of the issuance and management of an End-Entity Certificate, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Certificate manufacturing process,
- The publication of Certificates,
- The revocation of Certificates,
- Ensuring that all aspects of the services, operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Certificate Status Authority (CSA)

A CSA is an authority that provides status of Certificates or certification paths. A CSA can be operated in conjunction with the CAs or independent of the CAs; for example, this can be an Online Certificate Status Protocol (OCSP) Responder that provides the revocation status of a specific Air Canada PKI-issued certificate upon request.

CSAs that are keyless and simply repeat responses signed by other CSAs shall adhere to the same security requirements as repositories.

An Air Canada Root CA must not provide certificate status via a CSA.

1.3.1.8 Card Management System (CMS)

The Card Management System is responsible for managing smart card token content.

1.3.1.9 Administration Workstation

Administration Workstations may be used to administer CA, CMS and CSA equipment and/or associated HSM from a specific secure location inside or outside the security perimeter of the CA, CMS and CSA. The Administration Workstation located outside the security perimeter is considered to be a logical extension of the secure enclave in which the CA, KES, CMS and CSA equipment reside.

1.3.2 Registration Authorities

An RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into her Public Key Certificate. An RA interacts with the CA to enter and approve the Subscriber Certificate request information.

The Air Canada Operational Authority acts as the RA for the Air Canada Root CAs, and for Air Canada PCAs when dealing with cross certification. It performs its function in accordance with the concerned Air Canada CPS approved by the Air Canada PMA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a Certificate, who asserts that it uses its key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and who does not itself issue Certificates.

Air Canada Root CA Subscribers shall include only Air Canada PKI CA Operational Authority personnel and, when determined by the Air Canada PMA, possibly certain network or hardware devices such as firewalls and routers when needed for PKI-infrastructure protection.

Air Canada Subordinate CA Subscribers shall include Air Canada employees, subcontractor personnel, suppliers, partners, customers, customers' customers, and hardware devices such as firewalls, routers, servers, or aircraft and/or aircraft equipment.

CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who are issued Certificates for uses other than signing and issuing Certificates or Certificate status information.

1.3.3.1 Affiliated Organisations

Subscriber certificates may be issued in conjunction with an organisation that has a relationship with the Subscriber; this is termed affiliation. The organisational affiliation shall be indicated in a relative distinguished name in the subject field in the certificate, and the certificate shall be revoked in accordance with Section 4.9.1 when affiliation is terminated.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a Public Key. The Relying Party is responsible for deciding how to check the validity of the Certificate by checking the appropriate Certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the Certificate. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.5 Other participants

1.3.5.1 Related Authorities

The Air Canada CAs operating under this CP may require the services of other security,

community, and application authorities, such as compliance auditors and attribute authorities. The Air Canada CPSes shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.5.2 Trusted Agent

- A Trusted Agent is appointed by the OA and may collect and verify Subscriber identity and information on behalf of an RA. Information shall be verified in accordance with section 3.2 and communicated to the RA in a secure manner.
- A Trusted Agent shall not have privileged access to the CA to enter or approve Subscriber information.

1.3.6 Applicability

The sensitivity of the information processed or protected using Certificates issued by Air Canada CAs will vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at various levels of assurance as listed in section 1.2.

The Certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance Level	Applicability
basic-software-256	This level is relevant to environments where risks and consequences of data compromise are low. Subscriber Private Keys shall be stored in software at this Assurance Level.
basic-hardware-256	This level is relevant to environments where risks and consequences of data compromise are low. Subscriber Private Keys shall be stored in hardware at this Assurance Level.
medium-software-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in software at this Assurance Level. Except for specific exceptions documented in this policy, only persons can be Subscribers of certificates that assert this assurance level OID.

medium-hardware-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in hardware at this Assurance Level. Except for specific exceptions documented in this policy, only persons can be Subscribers of certificates that assert this assurance level OID.
medium-software-device-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in software at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.
medium-hardware-device-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in hardware at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.
BEGSS	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in software at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.
BEGSS-hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in hardware at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.

E-EGS	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in software at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.
E-EGS-hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in hardware at this Assurance Level. Only non-person entities (i.e. devices) can be Subscribers of certificates that assert this assurance level OID.

1.3.6.1 Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the Certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the Air Canada PMA or the Air Canada Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth herein, which Relying Parties may consider in making their decisions.

1.3.6.2 Obtaining Certificates

Relying Parties see section 2.

All other entities see section 3.

1.4 Certificate Usage

The Air Canada CAs will issue digital Certificates to Subscribers for various uses. Examples include:

- Establishment of encrypted communication links (IPsec VPN)
- Authentication to IT systems
- Signing digital documents
- Encrypting and decrypting digital documents

This list of use cases for digital Certificates issued by Air Canada CAs is not complete and may be extended.

Certificates are also issued as needed to PKI infrastructure devices and/or personnel.

Certificates asserting the -256 assurance levels shall be only issued using the SHA256 hash algorithm.

1.4.1 Appropriate Certificate uses

No stipulation.

1.4.2 Prohibited Certificate uses

Prohibited applications include the following:

- any export, import, use or activity that contravenes any local or international laws or regulations;
- any usage of Certificates in conjunction with illegal activities;
- any usage of Certificates for personal use or purposes not related to the Community's business;
- any use of a Certificate after it has been suspended or revoked.

The Subscriber and/or Subscriber's Employer that uses a Certificate for a prohibited application shall be liable as set out in section 9 for such use and its consequences, which may include the revocation of the Certificate(s)."

1.5 POLICY ADMINISTRATION

1.5.1 Organisation administering the document

The Air Canada PMA is responsible for all aspects of this CP.

1.5.2 Contact person

Questions regarding this CP shall be directed to the Air Canada PMA represented by:

Shaun Harrison
Director, Cybersecurity Operations
Chair of the Air Canada PKI PMA

Air Canada Hangar 101
8050 22 St NE, Calgary, AB
Canada
T2E 7Z6
shaun.harrison@aircanada.ca

1.5.3 Person determining CPS suitability for the policy

The Air Canada PMA shall commission an analysis to determine whether the Air Canada PKI CPSes conform to the Air Canada PKI CP.

When such a compliance analysis shall be performed:

- The determination of suitability shall be based on an independent compliance analyst's results and recommendations; and
- The compliance analysis shall be from a firm, which is independent from the entity being audited. The compliance analyst may not be the author of the CP or the CPS; and
- The entity PMA shall determine whether a compliance analyst meets these requirements.

When entering into a MOA:

- Each entity shall be responsible for determining whether their CPS(s) conform to their CP(s).
- Entities shall be obliged to properly adhere to the policy mapping between the Air Canada PKI CP and external PKI domain CPs.
- The entity shall be obliged to attest to such compliance periodically.

1.5.4 CPS approval procedures

The CPS shall be more detailed than the corresponding Certificate Policy described in this document. The Air Canada PKI CPSes shall specify how this CP shall be implemented to ensure compliance with the provisions of this CP. The approval procedures for the CPSes shall be outlined in the Air Canada PMA Charter and by-laws.

1.5.5 Waivers

There shall be no waivers to this CP.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Accreditation - Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Activation Data - Secret data (e.g.: password, PIN code) that is used to perform cryptographic operations using a Private Key.

Air Transport Association of America (ATA) – An American trade association and lobbying group that represents the largest US airlines. Now known as Airlines for America (A4A).

Assurance Level - A representation of how well a Relying Party can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the End-Entity whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was used to produce the Certificate and (if appropriate) deliver the Private Key to the End-Entity performs its task.

Authority Revocation List (ARL) - A list of revoked Certification Authority Certificates.

Technically, an ARL is a CRL; all requirements applicable to CRLs also apply to ARLs.

Authentication - The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.

Audit - An Independent review and examination of documentation, records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Certificate - A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information:

- The identity of the Certification Authority issuing it.
- The identity of the certified End-Entity.
- A Public Key that corresponds to a Private Key under the control of the certified End-Entity.
- The Operational Period.
- A serial number.

The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.

Certification Authority (CA) - A Certification Authority is an entity that is responsible for authorising and causing the issuance or revocation of a Certificate.

By extension, the term "CA" can also be used to designate the infrastructure component that technically signs the Certificates and the revocation lists it issues.

A Certification Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities.

A Certification Authority performs three essential functions. First, it is responsible for identifying and authenticating the intended Authorised Subscriber to be named in a Certificate, and verifying that such Authorised Subscriber possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate. Second, the Certification Authority actually creates and digitally signs the Authorised Subscriber's Certificate. The Certificate issued by the Certification Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private Key Pair. Third, the Certification Authority creates and digitally signs the Certificate Revocation Lists and/or Authority Revocation Lists.

Certificate Extension - A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.

Certificate Manufacturing - The process of accepting a Public Key and identifying information from an authorised Subscriber; producing a digital Certificate containing that and other pertinent information; and digitally signing the Certificate.

Certificate Policy (CP) - A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of applications with common security requirements.

Within this document, the term CP, when used without qualifier, refers to the Air Canada

CP, as defined in section 1.

Certification Practice Statement (CPS) - A statement of practices which a CA employs for issuing and revoking Certificates and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.

Certificate Request - A message sent from an applicant to a CA in order to apply for a digital Certificate. The Certificate request contains information identifying the applicant and the Public Key chosen by the applicant. The corresponding Private Key is not included in the request, but is used to digitally sign the entire request.

If the request is successful, the CA will send back a Certificate that has been digitally signed with the CA's Private Key.

Certificate Revocation List (CRL) - A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs.

When an End-Entity chooses to accept a Certificate, the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.

Certificate Status Authority (CSA) - A CSA is an authority that provides status of Certificates or certification paths.

Cross-Certificate (CC) - A Certificate used to establish a trust relationship between two Certification Authorities.

A Cross-Certificate is a Certificate issued by one CA to another CA which contains the subject CA Public Key associated with the private CA signature key used by the subject CA for issuing Certificates. Typically, a Cross-Certificate is used to allow End-Entities in one CA domain to communicate securely with End-Entities in another CA domain. A Cross-Certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1 domain, to accept a Certificate used by Entity #b, who has a Certificate issued to Entity #b by CA#2.

Digital Security Working Group (DSWG) – A group of the ATA e-Business Program tasked with providing a forum to address the application of digital data security technologies and standards to ATA e-Business specifications.

Digital Signature - The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine:

- Whether the transformation was created using the private signing key that corresponds to the signer's public verification key; or
- Whether the message has been altered since the transformation was made.

Directory - A directory system that conforms to the ITU-T X.500 series of Recommendations.

Distinguished Name - A string created during the certification process and included in

the Certificate that uniquely identifies the End-Entity within the CA domain.

Encryption Key Pair - A public and private Key Pair issued for the purposes of encrypting and decrypting data.

End-Entity (EE) - A person, device or application that is issued a Certificate by a CA.

Entity - Any autonomous element within the PKI, including CAs, RAs and End-Entities.

Employee - An employee is any person employed in or by Air Canada.

Federal Information Processing Standards (FIPS) - Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.

Hardware Token - A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorisation. Smart cards and USB tokens are examples of hardware tokens.

Hardware Security Module (HSM) - An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (End-Entities).

Internet Engineering Task Force (IETF) - The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Intermediate CA - A CA that is not a Root CA and who issues Certificates to other CAs within the same PKI. An Intermediate CA is a Subordinate CA.

Issuing CA - In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the Certificate.

Key Ceremony – A planned, exceptional event during which a Certification Authority is used to perform a non-trivial activity, such as the generation of its own Key Pair, the generation of its own Certificate Request, the issuance of a Certificate or the generation of revocation lists for off-line CAs. The ceremony is usually documented in advance and in detail in a Key Ceremony Script.

Key Ceremony Script - The detailed, keystroke-level procedure to be followed during the Key Ceremony.

Key Generation - The process of creating a Private Key and Public Key pair.

Key Pair - Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.

Memorandum of Agreement - As used in the context of this CP, between Air Canada or an Air Canada Business Unit and external PKI Domains legal Representation allowing interoperation between the respective Air Canada PKI CAs and an external PKI domains

CA.

Air Canada consults the Air Canada PMA through the Air Canada PMA Chair on the MOA.

Online Certificate Status Protocol (OCSP) - Protocol useful in determining the current status of a digital Certificate without requiring CRLs.

Object Identifier (OID) - An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognised standards organisation.

Operational Authority (OA) - An agent of the Air Canada PKI CA. The Operational Authority is responsible to the Policy Management Authority for:

- Interpreting the Certificate Policies that were selected or defined by the Policy Management Authority.
- Developing a Certification Practice Statement (CPS), in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647), to document the CA's compliance with the Certificate Policies and other requirements.
- Maintaining the CPS to ensure that it is updated as required.
- Operating the Certification Authority in accordance with the CPS.

Operational Period of a Certificate - The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.

Organisation - Department, agency, partnership, trust, joint venture or other association.

Person - A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.

PIN - Personal Identification Number. See activation data for definition.

PKI Disclosure Statement (PDS) - Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasising information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS."

PKIX - IETF Working chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.

Policy - This Certificate Policy.

Policy Management Authority (PMA) - An agent of the Certification Authority. The Policy Management Authority is responsible for:

- Dispute resolution.
- Selecting and/or defining Certificate Policies, in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647), for use in the Certification Authority PKI or organisational enterprise.
- Approving of any interoperability agreements with external Certification Authorities.

- Approving practices, which the Certification Authority must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies.
- Providing Policy direction to the CA and the Operational Authority.

Public Key Infrastructure (PKI) - A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.

Principal CA (PCA) - CA within a PKI that has been designated to interoperate directly with another PKI (e.g., through the exchange of Cross-Certificates with a PCA in another PKI domain).

Private Key - The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.

Public Key - The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.

Public/Private Key Pair - See Key Pair.

Registration - The process whereby a user applies to a Certification Authority for a digital Certificate.

Registration Authority (RA) - An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party (RP) - A Relying Party is a recipient of a Certificate signed by the Air Canada PKI CA who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS.

The term "Relying Party" designates the legal entity responsible for the recipient's actions.

Relying Party Agreement - An agreement, entered into by a Relying Party that provides for the respective liabilities of Air Canada or its Business Units and of the Relying Party. Such agreement is a prerequisite in order to be able to rely on the Certificate.

Repository - Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).

Revocation - To prematurely end the Operational Period of a Certificate from a specified time forward.

RFC 3279 - Document published by the IETF which "[…] specifies algorithm identifiers and ASN.1 encoding formats for digital signatures and subject public keys used in the Internet X.509 PKI" (RFC 3279).

RFC 3647 - Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and

communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.

RFC 4122 – Document published by the IETF which "[…] defines a Uniform Resource Name namespace for UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique IDentifier)". (RFC 4122)

RFC 5280 – Document published by the IETF which "[…] profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet." (RFC 5280)

Role Certificate - A Role Certificate is a Certificate which identifies a specific role on behalf of which the human Subscriber is authorised to act.

Root CA - A CA that is the trust anchor for a set of relying parties.

Server-based Certificate Validation Protocol (SCVP) - Protocol that allows a client to delegate Certificate path construction and Certificate path validation to a server.

Secure Signature-Creation Devices (SSCD) - A set of hardware and software elements designed for and allowing the creation of a digital signature in a secure manner. This is used in the context of the CEN CWA 14169 standard.

Signature Key Pair - A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.

Signing CA - A CA whose primary function is to issue Certificates to End-Entities. A Signing CA is a Subordinate CA.

Software-based Certificate - A digital Certificate (and associated Private Keys) that are created and stored in software – either on a local workstation or on a server.

Spec 42 – The Aviation Industry Standards for Digital Information Security, maintained by the DSWG.

Sponsoring Organisation - An organisation with which an Authorised Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).

Subordinate CA - A CA that is not a Root CA. It is subordinate to either a Root CA or other Subordinate CA.

Subscriber - An entity that is the subject of a Certificate and which is capable of using, and is authorised to use, the Private Key, that corresponds to the Public Key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the Certificate Policy and the Subscriber Agreement.

Subscriber Agreement - An agreement, entered into by a Subscriber that provides the responsibilities and obligations of the Subscribers when using Certificates. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.

Time-Stamp Authority (TSA) - An authority that issues and validates trusted timestamps.

Token - A hardware security device containing an End-Entity's Private Key(s) and Certificate. (see "Hardware Token")

Trusted Agent - An agent who a Registration Authority relies on to verify that an applicant

fulfils part of or all of the necessary prerequisites to obtain a Certificate for an End-Entity.

Trustworthy System - Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate - A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

X.509 - An ITU-T standard for a Public Key Infrastructure.

1.6.2 Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One Encoder / Decoder
ATA	Air Transport Association of America
AW	Administration Workstation
BEGSS	Boeing e-Plane Ground Support System
C	Country
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name Service
DSWG	Digital Security Working Group
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End-Entity
E-EGS	E-Enabling Ground System

FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
GUID	Globally Unique Identifier
HR	Human Resources
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
KES	Key Escrow System
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol
LSAP	Loadable Software Airplane Parts or Loadable Software Aircraft Parts
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	Organisation
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisational Unit
PCA	Principal Certification Authority
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority

RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCVP	Server-based Certificate Validation Protocol
SHA-1	Secure Hash Algorithm, Version 1
SSCD	Secure Signature-Creation Devices
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TSA	Time-Stamp Authority
UPN	User Principal Name
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

2 Publication and Repository Responsibilities

2.1 Repositories

The Air Canada PKI operates Repositories containing all information necessary to provide validation services for issued Certificates.

The mechanisms used by the Air Canada PKI to post information to its respective Repositories, as required by this CP, shall include:

- A publication service accessible via the Internet through the Hypertext Transport Protocol (HTTP); and
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP; and
- Access control mechanisms when needed to protect repository information, as described in later sections.

The PKI Repositories containing CA Certificates and Certificate status information shall be deployed so as to provide high levels of reliability (24 out of 24 hours, 7 out of 7 days at a rate of 99% availability or better).

2.2 Publication of Certificate information

2.2.1 Publication of CA Information

The Air Canada PKI CP shall be published electronically on the Air Canada PKI web site.

All encryption Public Key Certificates issued by the Air Canada CAs to Subscribers shall be published to the applicable Air Canada Repositories, as set forth in the applicable CPSes.

All CRLs, ARLs, CA Certificates, and CA Cross-Certificates issued by Air Canada CAs shall be published to the respective and applicable Repositories as set forth in the applicable CPSes. Furthermore, all of the above shall be accessible via HTTP.

The applicable Certificate Practice Statements shall be kept confidential and shall not be published publicly with, or separate from, this CP.

All publication made by Air Canada CAs shall be performed as soon as an internal event that may require publication (revocation, issuance, or modification of a Certificate) is validated by the CA.

2.2.2 Interoperability

The Air Canada PKI shall not publish CA Certificates, CA Cross-Certificates and CRLs in an LDAP directory.

2.2.3 Privacy of Information

Air Canada PKI CAs and RAs shall respect the privacy of Subscribers and Subscriber's Employers, as described in section 9.4.

2.3 Time or frequency of publication

Air Canada PKI CA public information identified in section 2.2.1 shall be published prior to the first Certificate being issued in accordance with this CP. CA Certificates and Certificate status information shall be published as specified in section 4 of this CP.

2.4 Access controls on Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected.

Status information for all Certificates shall be publicly available through the Internet.

Encryption Certificates for which publication is required shall be publicly available through the Internet.

This CP shall be publicly available through the Internet.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The Air Canada CAs shall generate and sign Certificates containing an X.501 Distinguished Name (DN) in the Issuer and Subject fields. Such DNs shall be assigned in accordance with section 3.1.4. Subject Alternative Name may be used, if marked non-critical; section 10 lists the accepted contents (email address, UPN, FQDN, etc.) and their specific formats.

For Certificates issued to human Subscribers, the subject DN shall either contain the affiliated organisation name in an appropriate relative distinguished name attribute (e.g., organisation (o), organisational unit (ou), or domain component (dc) attribute) or shall contain the value "Unaffiliated" in the last organisational unit (ou) attribute.

3.1.2 Need for names to be meaningful

The Certificates issued pursuant to this CP are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates shall identify the person or object to which they are assigned in a meaningful way.

DNs shall be used, wherein the Common Name represents the Subscriber in a way that is easily understandable for humans.

- For people, this will typically be:

  Given-Name[space][2]Surname, and subject to the uniqueness requirements of section 3.1.5).

- For equipment:

  This may include an IP address, a Fully-Qualified Domain Name (FQDN), a URL, or an otherwise human-understandable unique identifier.

- For Roles:

  This shall be a clear representation of the role (e.g.: Purchasing Agent, System Administrator, Final Quality Assurance Engineer, etc.);

An Air Canada Root CA shall impose restrictions on the name space authorised to that Air Canada Subordinate CA which are at least as restrictive as its own name constraints.

All DNs shall be unique and shall satisfy asserted namespace constraints.

Subject DNs shall accurately reflect the organisation with which the Subject is affiliated.

When UPNs are used, they shall be unique and accurately reflect organisational structure.

[2] "[space]" refers to a space character and not the individual characters.

3.1.3 Anonymity or pseudonymity of Subscribers

CA Certificates shall not contain anonymous or pseudonymous identities.

Certificates issued by Air Canada CAs shall not contain anonymous or pseudonymous identities, only names as defined in section 7 and as stipulated in section 3.1.2.

3.1.4 Rules for interpreting various name forms

Rules for interpreting name forms shall be contained in the [Air Canada DIT], and in the applicable Certificate profile.

The authority responsible for Air Canada PKI name space control is the Air Canada PMA.

3.1.5 Uniqueness of names

Name uniqueness across the Air Canada PKI name space domains shall be enforced. The Air Canada CAs and RAs shall enforce name uniqueness within their authorised X.500 name space.

The applicable CPSes shall describe how names shall be allocated within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if "Joe Q Smith" leaves a CA's community of Subscribers, and a new, different "Joe Q Smith" enters the community of Subscribers, how will these two people be provided unique names).

The Air Canada PMA shall be responsible for ensuring name uniqueness in Certificates issued by the Air Canada CAs.

3.1.6 Recognition, authentication, and role of trademarks

The use of trademarks will be reserved to registered trademark holders and to the CAs in strict proportion to that required for the performance of this CP.

3.1.7 Name Claim Dispute Resolution Procedure

The Air Canada PMA shall resolve or cause to be resolved any name collision brought to its attention that may affect interoperability.

3.2 Initial Identity Verification

3.2.1 Method to prove possession of Private Key

In all cases where the party named in a Certificate generates its own keys, that party shall be required to prove possession of the Private Key, which corresponds to the Public Key in the Certificate request. For signature keys, this may be done by the entity using its Private Key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party's Public Key. The Air Canada PMA may allow other mechanisms that are at least as secure as those cited here.

In the case of a Device that is not capable of generating its own keys, this may only be possible from a separate computer before the key is transferred onto the Device. Subsequent to proof of possession, the private key shall be distributed to the Device in a

manner consistent with section 6.2.

3.2.2 Authentication of organisation identity

In all cases, the existence of an affiliated organisation shall be verified prior to issuing an end user Certificates on its behalf. Moreover, requests for end user Certificates other than unaffiliated Subscribers shall include the name of the organisation and shall be verified with the identified affiliated organisation.

The verification shall include the following:

- Full organisation name;
- Address of its head office;
- Documentation of the existence of the organisation (such as articles of incorporation or corporation number);
- Its Dun and Bradstreet (DUNS) identifier, if doing business within the United States of America or elsewhere where this identifier is commonly used. If a DUNS identifier is not able to be provided, the Entity CA shall verify with another third party (e.g. Tax authority, country, state or province corporate registry) the existence of the company, and record that identifier;
- A letter from its authorised representative officially requesting said Certificate.

The RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorisation to act in the name of the organisation.

Requests for Cross-Certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing Cross-Certificates, the issuing CA shall verify the information provided, in addition to the authenticity of the requesting representative and the representative’s authorisation to act in the name of the CA.

3.2.3 Authentication of individual identity

The Air Canada CAs shall ensure that the applicant’s identity information is verified and checked in accordance with this CP and the applicable CPSes. The CA or an RA shall ensure that the applicant’s identity information and Public Key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each Certificate. Process information shall depend upon the Certificate level of assurance and shall be addressed in the applicable CPS.

3.2.3.1 Authentication of Individuals

CAs and RAs are responsible for ensuring that they are in compliance with all applicable laws when collecting personally identifiable information. If a jurisdiction prohibits the collection, distribution or storage of any of the information specified in this section, an alternate, equivalent proofing mechanism may be used that assures the identity of the applicant to an equivalent level, subject to approval of the Air Canada PMA. If the data is used to proof an identity for Medium Assurance Levels, this alternate procedure shall be

communicated to external domain PKIs prior to implementation, or as outlined in the MOA with that external domain PKI.

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification; and
- A signed declaration by that person that he or she verified the identity of the applicant as required by this CP which may be met by establishing how the applicant is known to the verifier as required by this CP, using the format set forth at 28 U.S.C. 1746 (Unsworn declarations under penalty of perjury) or comparable procedure under local law; the signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued.

For basic-256 Assurance Levels, the following information shall be recorded:

- the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
- the full name and legal status of the applicant's Employer;
- an email address for the applicant, if available;
- a declaration signed by the applicant indicating her acceptance of the privacy policy outlined in section 9.4;
- the date and time of the verification;

For all Assurance Levels applicable to human Subscribers other than Basic, the following information shall be recorded:

- the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
- the date and place of birth or other attribute(s) which may be used to uniquely identify the applicant;
- the full name and legal status of the Subscriber's Employer;
- a physical address or other suitable method of contact;
- a declaration signed by the applicant indicating her acceptance of the privacy policy outlined in section 9.4;
- a number or code allowing unambiguous identification of the verifier;
- a unique identifying number from an ID of the applicant;
- the date and time of the verification; and
- a declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note). This shall be performed in the presence of the person performing the identity authentication.

PRACTICE NOTE:

In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature Certificate is generated immediately upon authentication of

the applicant's identity, the applicant may sign the declaration of identity and Certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity then the Certificate must be revoked.

For Certificates asserting the Medium Assurance Levels, the applicant shall:

- present one (1) valid National Government-issued photo ID or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License). The verifier must be able to easily assess the authenticity, validity and contents of the ID presented by the applicant. If this is not possible, the ID must be rejected.

For Basic Assurance Level Certificates, the applicant's identity can be determined based on existing corporate or commercial data.

Identity for other Assurance Levels applicable to human Subscribers shall be established by in-person proofing before the RA or Trusted Agent; information provided shall be verified to ensure legitimacy.

Authentication of an individual's identity can also be performed using an in-person antecedent, i.e. an established trust relationship; this described in section 3.2.3.3.

If Subscriber credentials containing the Private Keys associated with the Public Key Certificates are lost, damaged or stolen, the Subscriber identity needs to be authenticated again as per the requirements of this section.

3.2.3.2 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) and other non-human Subscribers (aircraft and/or aircraft equipment/components/sub-components/systems, etc.) will be named as Certificate Subjects. In such cases, the component (usually referred to as a "Device", "non-person entity" or "NPE") shall have a human sponsor (the "Device Sponsor"). The Device Sponsor shall be responsible for providing the following registration information:

- Equipment identification (e.g. IP address, hostname, aircraft registration number, aircraft/equipment part number) or service name (e.g., DNS name) sufficient to unique identify the Subject;
- Equipment Public Keys;
- Equipment authorisations and attributes (if any are to be included in the Certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the Device Sponsor (using Certificates of equivalent or greater assurance than that being requested); or

- In-person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1.
- In the event a human sponsor is changed, the new sponsor shall review the status of each device under her sponsorship to ensure it is still authorised to receive Certificates. The CPS shall describe procedures to ensure that Certificate accountability is maintained.

3.2.3.3 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

The following requirements shall apply when human Subscriber identity is verified using antecedent relationship with the sponsoring organisation:

1. The applicant shall personally appear before a verifier (for example, a Trusted Agent); for fully and properly registered Air Canada employees, in-person proofing may be performed remotely via a live video link. This video link must be of a quality sufficient to allow the RA or Trusted Agent to unambiguously verify the applicant's identity and ensure the legitimacy of the presented ID.
2. The applicant and the verifier shall have an established working relationship with the sponsoring organisation. The relationship shall be sufficient to enable the verifier to, with a high degree of certainty, verify that the applicant is the same person that was identity proofed. An example to meet this requirement is when the applicant and verifier are employed by the same company and the company badge forms the basis for the applicant authentication;
3. The applicant shall present a valid sponsoring organisation-issued photo ID. This photo ID shall have been issued on the basis of in-person identity proofing using one valid National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License);
4. The verifier shall record the following:
    a. Number or code allowing unambiguous identification of the verifier;
    b. Unique identifying number from the applicant's sponsoring organisation-issued photo ID;
    c. Date and time of the identity verification; and
    d. Date and time of sponsoring organisation-issued photo ID, if applicable.
5. The verifier shall sign a declaration that he or she verified the identity of the applicant as required by the applicable Certificate Policy which may be met by establishing how the applicant is known to the verifier as required by this Certificate Policy; and
6. The applicant shall sign a declaration of identity using a handwritten signature or appropriate digital signature. This declaration shall be signed in the presence of the verifier.

3.2.3.4 Authentication of Human Subscriber for Role Certificates

Human Subscribers may be issued Role Certificates. In addition to the stipulations below, authentication of individuals for Role Certificates shall follow the stipulations of sections

3.2.3.1 of this CP.

A Role Certificate shall identify a specific role title on behalf of which the Subscriber is authorised to act rather than the Subscriber's name. A Role Certificate can be used in situations where non-repudiation is desired. A Role Certificate shall not be a substitute for an individual Subscriber Certificate. Each role for which a Role Certificate is to exist shall have one or more Role Sponsors.

Multiple Subscribers can be assigned to a role at the same time, however, the signature key pair shall be unique to each Role Signature Certificate issued to each individual; the encryption key pair and Role Encryption Certificate may be shared by the individuals assigned the role.

The CA or the RA shall record the information identified in Section 3.2.3.1 for a Role Sponsor associated with the role before issuing a Role Certificate. The CA or the RA shall validate from the Role Sponsor that the individual Subscriber has been approved for the Role Certificate.

Subscribers issued Role Certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing Role Certificates shall comply with all other stipulations of this CP (e.g., Subscriber identity proofing, validation of organisation affiliation, key generation, private key protection, and Subscriber obligations).

The individual assigned the role or the Role Sponsor may act on behalf of the Certificate subject for Certificate management activities such as:

- Issuance;
- Re-key; and
- Revocation.

Issuance of Role Signature Certificates shall require the approval of the Role Sponsor. Renewal and re-key shall require the approval of the Role Sponsor if the validity period is extended beyond that already approved by the Role Sponsor. Role Sponsors are defined in section 5.2.1.

3.2.4 Non-verified Subscriber information

Information that is not verified shall not be included in Certificates.

3.2.5 Validation of authority

Prior to issuing Cross-Certificates, the Issuing Air Canada PCA shall validate the external PKI domain CA Certificate requestor's authorisation to act in the name of the external PKI domain CA. In addition, the Air Canada PCA shall obtain Air Canada PMA approval prior to issuing CA Certificates.

Certificates that contain explicit or implicit organisational affiliation shall be issued only after ascertaining that the applicant has the authorisation to act on behalf of the organisation in the asserted capacity.

For Certificates which are to be loaded in aircraft avionics, a document proving the

Applicant's employer's status as an airline or as another type of legitimate operator of the given aircraft, such as a copy of aircraft registration documents, must be provided.

For Certificates used by ground entities that communicate with aircraft avionics, a document proving the Applicant's employer's status as an airline as above, or as a supplier of datalink service to an airline, such as a signed contract to that effect, must be provided.

For all Code Signing Certificates, a document must be provided, proving the Subscriber's right to create and publish software within the community.

3.2.6 Criteria for interoperation

Air Canada PCAs implementing this CP shall certify other CAs (including cross-certification) only as authorised by the Air Canada PMA. Such an external PKI domain CA shall adhere to the following requirements before being approved by the Air Canada PMA for cross-certification:

- Have a CP mapped to and determined by the Air Canada PMA to be in conformance with this CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to section 8 of this CP and as set forth in the Subject CA CP;
- Issue Certificates compliant with the profiles described in this CP, and make Certificate status information available in compliance with this CP;
- Provide CA Certificate and Certificate status information to the Relying Parties in compliance with this CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key

External PKI domain CAs and Subscribers shall be authenticated through use of their current public key Certificates or by using the initial identity-proofing process as described above in section 3.2.

Re-key of CAs other than External PKI domain CAs is not permitted.

Further identification and authentication requirements apply according to the Assurance Level, as set forth in the table below.

Assurance level	Further requirements
basic-software-256 basic-hardware-256	No further requirements
medium-software-256 medium-hardware-256 medium-device-software-256 medium-device-hardware-256 BEGSS BEGSS-hardware	The initial identity-proofing process must be carried out at least once every nine (9) years

E-EGS E-EGS-hardware	

For external PKI domain CAs, identity shall be re-established through the initial registration process at least once every three (3) years as required by section 3.2.2.

When a current Public Key Certificate is used for identification and authentication purposes, the expiration date of the new Certificate shall not cause the Certificate Subject to exceed the initial identity-proofing time frames specified in the table and paragraph above, and the assurance level of the new Certificate shall not exceed the assurance level of the Certificate being used for identification and authentication purposes.

3.3.2 Identification and authentication for re-key after revocation

After a Certificate has been revoked other than during an update action, the subject (i.e., a CA or an End-Entity) is required to go through the initial registration process described in section 3.2 to obtain a new Certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests shall always be authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's associated Public Key, regardless of whether the Private Key has been compromised.

4 Certificate Life-cycle Operational Requirements

It is the intent of this CP to identify the minimum requirements and procedures that are necessary to support trust in the PKI, and to minimise imposition of specific implementation requirements on the OA, Subscribers, and Relying Parties.

Communication among the CA, RA, Trusted Agent, other parties confirming identities, and Subscriber shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the Assurance Level of the Certificate being managed. When cryptography is used, the mechanism shall be at least as strong as the Certificates being managed. For example, a web site secured using SSL Certificate issued under medium-software-256 policy and set up with appropriate algorithms and key sizes satisfies integrity and confidentiality requirements for medium-software-256 Certificate management.

The content of communication shall dictate if some, all, or none of the security services are required.

4.1 Certificate Application

4.1.1 Who can submit a Certificate application

4.1.1.1 Application for End-Entity Certificates by an individual

The Subscriber or RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.2 Application for End-Entity Certificates on behalf of a device

The Device Sponsor, who needs to be a Subscriber, or an RA acting on behalf of the Subscriber, shall submit a Certificate application to the CA.

4.1.1.3 Application for CA Certificates

For the Certificate applications a CA makes to an Air Canada Root or PCA, an authorised representative of the Subject CA shall submit the application to the Air Canada PMA.

4.1.2 Enrolment process and responsibilities

Applicants for Public Key Certificates shall be responsible for providing accurate information in their applications for certification.

Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties, and shall be described in the applicable CPS.

For CA Certificates, the Air Canada PMA shall verify all authorisations and other attribute information received from an applicant CA.

4.1.2.1 End-Entity Certificates

The applicant and the RA must perform the following steps when an applicant applies for

a Certificate:

- establish and record identity of Subscriber (per section 3.2);
- obtain a public/private Key Pair for each Certificate required; and
- establish that the Public Key forms a functioning Key Pair with the Private Key held by the Subscriber (per section 3.2.1).
- provide a point of contact for verification of any roles or authorisations requested; and
- verify the authority of the applicant.

These steps may be performed in any order that is convenient for the RA and Subscribers, and that do not defeat security; but all must be completed prior to Certificate issuance.

Any electronic transmission of shared secrets shall be protected (e.g., encrypted, or using a split secret scheme where the parts of the shared secret are sent using multiple, separate channels) using means commensurate with the requirements of the data to be protected by the Certificates being issued.

4.1.2.2 CA Certificates

The Air Canada PMA shall make the procedures and application form available to entities requesting issuance of a CA Certificate from an Air Canada Root or PCA.

An Air Canada Root CA shall certify Air Canada Subordinate CAs implementing this CP only as authorised by the Air Canada PMA. A CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647], shall accompany the applications of the requesting Air Canada Subordinate CA.

Requests by external PKI domain CAs for CA Certificates from an Air Canada PCA shall be submitted to the Air Canada PMA using the contact provided in section 1.5.

The Air Canada PMA shall evaluate the submitted application in accordance with procedures that it shall develop and publish, and make a determination regarding whether to issue the requested Certificate(s), and what policy mapping to express in the Certificate(s), if applicable[3].

The Air Canada PMA shall commission a CPS compliance analysis prior to authorising the OA to issue and manage CA Certificates asserting this CP.

Air Canada CAs shall only issue Certificates asserting the OIDs outlined in this CP upon receipt of written authorisation from the Air Canada PMA, and then may only do so within the constraints imposed by the Air Canada PMA or its designated representatives.

4.2 Certificate application processing

It is the responsibility of the RA, or, in the case of a CA Certificate, the Air Canada PMA, to verify that the information in a Certificate Application is accurate.

This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal

[3] Note that subordinated CAs (Air Canada Subordinate CAs) inheriting this CP do not require policy mapping.

contact with the Subscriber's sponsoring organisation. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorised modification to a level commensurate with the level of assurance of the Certificate being sought.

Specifically, the databases shall be protected using physical security controls, personnel security controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

The applicable CPS shall specify procedures to verify information in Certificate Applications.

4.2.1 Performing identification and authentication functions

Prior to Certificate issuance, a Subscriber shall be required to sign a Subscriber Agreement containing the requirements that the Subscriber shall protect the Private Key and use the Certificate and Private Key for authorised purposes only.

4.2.2 Approval or rejection of Certificate applications

The Air Canada CAs, respective RAs, or the Air Canada PMA may approve or reject a Certificate application.

For CAs, the Air Canada PMA may approve or reject a Certificate application.

4.2.3 Time to process Certificate applications

The Certificate application processing from the time the request/application is posted on the CA or RA system to Certificate issuance shall take no more than 30 days.

4.3 Certificate Issuance

Upon receiving a request to issue a Certificate, the CA shall ensure that there is no deviation in the requested attributes from the information validated as per section 4.2.

The Certificate request may contain an already built ("to-be-signed") Certificate. This Certificate must not be signed until the process set forth in this CP and the respective CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the CA and the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, through other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organisation. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorised modification to a level commensurate with the level of assurance of the Certificate being sought.

Specifically, the databases shall be protected using appropriate physical security controls, personnel security controls, cryptographic security controls, computer security controls, and/or network security controls specified for the RA elsewhere in this CP to a level commensurate with the level of assurance of the Certificate being sought.

4.3.1 CA actions during Certificate issuance

The CA verifies the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.

The CA shall authenticate a Certificate Request, ensure that the Public Key is bound to the correct Subscriber, obtain a proof of possession of the Private Key, then generate a Certificate, and provide the Certificate to the Subscriber. When applicable, the CA shall publish the Certificate to the repository as described in section 2 of this CP and in the applicable CPS, after generation, verification, and acceptance.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

The CA shall notify Subscribers of successful Certificate issuance in accordance with procedures set forth in the applicable CPS.

The Air Canada OA shall inform the Air Canada PMA of any Certificate issuance to a CA by an Air Canada Root or PCA. The Air Canada PMA shall inform the authorised instance of such applicant CA of the successful Certificate issuance.

Notification of Certificate issuance shall be provided to the Air Canada CAs and to cross-certified PKI domains' PMAs according to the contractual obligations established through the respective MOA by the Air Canada PMA.

4.4 Certificate Acceptance

Air Canada shall enter into a Memorandum of Agreement (MOA) with external PKI domains' legal representatives setting forth the respective responsibilities and obligations of both parties. The acceptance procedure for the respective CA Certificates shall be defined in the MOA.

4.4.1 Conduct constituting Certificate acceptance

As part of the Certificate issuance process, a Subscriber shall explicitly indicate acceptance or rejection of the Certificates to the CA as set forth in the respective CPS, with the exception of Certificates issued to Devices at a Basic Level of Assurance, where explicit acceptance is not required.

For the issuance of CA Certificates to Air Canada Subordinate CAs, the Air Canada PMA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

4.4.2 Publication of the Certificate by the CA

Certificates shall be published according to section 2 as soon as they are issued.

4.4.3 Notification of Certificate issuance by the CA to other entities

The Air Canada OA shall inform the Air Canada PMA of any cross Certificate issuance to an external PKI domain CA by an Air Canada PCA.

The Air Canada PMA shall inform the authorised representative of such applicant external PKI domain CA of the successful cross-Certificate issuance.

Notification of such cross-Certificate issuance shall be provided to the Air Canada CAs and to cross-certified PKI domains' PMAs according to the contractual obligations established through the respective MOA by the Air Canada PMA.

4.5 Key pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate usage

Subscribers and CAs shall protect their Private Keys from access by any other party, as specified in section 6.2. Use of the Private Key corresponding to the Public Key in the Certificate, aside from initial proof-of-possession transaction with the CA, shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the Certificate.

Subscribers and CAs shall use their Private Keys for the purposes as constrained by the extensions (such as key usage, extended key usage, Certificate Policies, etc.) in the Certificates issued to them. For example, the OCSP Responder Private Key shall be used only for signing OCSP responses.

4.5.2 Relying Party Public Key and Certificate usage

Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess the following:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by section 1.4.1 or 1.4.2. CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate;
- that the Certificate is being used in accordance with the keyUsage, extendedKeyUsage, and certificatePolicies field extensions included in the Certificate; and
- the status of the Certificate and all Certificates in the chain of trust, including revocation status according to section 4.9.6.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilise appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate chain and verifying the digital signatures on all Certificates in the Certificate chain.

4.6 Certificate Renewal

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, with a new extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are

unchanged. After Certificate renewal, the old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Certificate Renewal shall only be supported for OCSP Certificates, CA Cross-Certificates, or Certificates where the Certificate Lifetime is shorter than the Private Key lifetime.

4.6.1 Circumstance for Certificate renewal

A Certificate may be renewed if the Public Key has not reached the end of its validity period, the associated Private Key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the Certificate must not exceed the remaining lifetime of the Private Key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2 Who may request renewal

An external PKI domain's PMA may request renewal of its cross Certificate.

A Device Sponsor may request renewal of an OCSP Certificate.

The PMA may request renewal of a PCA's Cross-Certificates.

4.6.3 Processing Certificate renewal requests

A Certificate renewal shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

For Cross-Certificates issued by an Air Canada PCA, Certificate renewal also requires that a valid MOA exists between the Air Canada PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new Certificate.

4.6.4 Notification of new Certificate issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate issuance by the CA to other entities

See Section 4.4.3.

4.7 Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery.

Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a Certificate means that a new Certificate is created that has the characteristics and assurance level as the old one, except that the new Certificate has a new, different Public Key (corresponding to a new, different Private Key) and a different serial number, and it may be assigned a different validity period.

After a re-key, the old Certificate shall not be further re-keyed, renewed, or modified. Additionally, the old Certificate shall be revoked, preferably with reason "superseded", if it is not expired.

4.7.1 Circumstance for Certificate re-key

A CA may issue a new Certificate to the Subject when the Subject has generated a new Key Pair and is entitled to a Certificate.

4.7.2 Who may request certification of a new Public Key

A Subject may request the re-key of its Certificate.

A Role Sponsor may request the re-key of a Role Signature, Role Identity or Role Encryption Certificate for which she is the sponsor.

The individual identified in a Role Signature or Role Identity Certificate may request the re-key of her Role Certificate

A Device Sponsor may request the re-key of a component Certificate they have sponsored.

An external PKI domain's PMA may request the re-key of its cross Certificate.

An Air Canada PKI CA may not request the re-key of its Certificate.

4.7.3 Processing Certificate re-keying requests

A Certificate re-key shall be achieved using one of the following processes:

- Initial registration process as described in section 3.2; or
- Identification & Authentication for Re-key as described in section 3.3.

For CA Certificates issued to other PKI domains' CAs, Certificate re-keying also requires that a valid MOA exists between Air Canada and the PMA of the respective other PKI domain CA, and the term of the MOA is beyond the expiry period for the new Certificate.

For Role Signature and Role Identity Certificates, re-key shall require the approval of the Role Sponsor if the validity period is extended beyond that already approved by the Role Sponsor.

4.7.4 Notification of new Certificate issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

See section 4.4.1 .

4.7.6 Publication of the re-keyed Certificate by the CA

See section 4.4.2 .

4.7.7 Notification of Certificate issuance by the CA to other entities

See section 4.4.3 .

4.8 Certificate Modification

Updating a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old Certificate. The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

This CP supports Certificate modification only for CA Certificates.

4.8.1 Circumstance for Certificate modification

A CA may issue a new Certificate to the Subject when some of the Subject information has changed and the Subject continues to be entitled to a Certificate.

4.8.2 Who may request Certificate modification

The PMA may request modification of an Air Canada CA Certificate.

An external PKI domain's PMA may request modification of its cross Certificate.

4.8.3 Processing Certificate modification requests

A Certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

For Cross-Certificates issued by an Air Canada CA, Certificate modification also requires that a valid MOA exists between the PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new Certificate.

4.8.4 Notification of new Certificate issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct constituting acceptance of modified Certificate

See Section 4.4.1

4.8.6 Publication of the modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate issuance by the CA to other entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A Certificate shall be revoked when the binding between the subject and the subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the Certificate become invalid;
- An organisation terminates its relationship with the CA such that it no longer provides affiliation information;
- Privilege attributes asserted in the Subject's Certificate are reduced;
- The Subject can be shown to have violated the stipulations of her agreement;
- The Private Key, or the media holding the Private Key, is suspected of compromise; or
- The Subject or other authorised party (as defined in this CP or the respective CPS) asks for her Certificate to be revoked.

Whenever any of the above circumstances occur, the associated Certificate shall be revoked and placed on the CRL. Revoked Certificates shall be included on all new publications of the Certificate status information until the Certificates expire.

In addition, if it is determined subsequent to issuance of new Certificates that a private key used to sign requests for one or more additional Certificates may have been compromised at the time the requests for additional Certificates were made, all Certificates authorised by directly or indirectly chaining back to that compromised key shall be revoked.

Air Canada PKI shall request that a cross-certified PKI domain's PMA revoke its cross Certificate if it does not meet the stipulations of the Certificate policies listed in the cross Certificate, including the cross-certified PKI domain' policy OIDs and "pass-through" policy OIDs.

4.9.2 Who can request revocation

A Certificate subject, human supervisor of a human subject, Human Resources (HR) person for the human subject, Device Sponsor for a component they have sponsored, issuing CA, or RA may request revocation of a Certificate.

For Role Signature and Role Identity Certificates, revocation may be requested by the individual identified in the Certificate or by the Role Sponsor. Role Encryption Certificate revocation may only be requested by the Role Sponsor.

In the case of CA Certificates issued to another PKI domain by an Air Canada PCA, the external PKI domain PMA or the Air Canada PMA may request revocation of a Certificate.

For CA Certificates, authorised individuals representing the CA Operational Authority may

request revocation of Certificates.

Notwithstanding the above, an Air Canada CA may, at its sole discretion, revoke any Subscriber or Device Certificate it has issued for reasons outlined in section 4.9.1.

4.9.3 Procedure for revocation request

A request to revoke a Certificate shall identify the Certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

Any CA may unilaterally revoke a CA Certificate it has issued. However, the Operational Authority for Air Canada CAs shall revoke a Subject CA Certificate only in the case of an emergency. Generally, the Certificate will be revoked based on the subject request, authorised representative of subject request, or PMA request.

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the Certificate. In the case of a CA Certificate issued by an Air Canada Root or PCAs, the Operational Authority shall seek guidance from the Air Canada PMA before revocation of the Certificate except when the Air Canada PMA is not available and there is an emergency situation such as:

- Request from the Subject CA for reason of key compromise;
- Determination by the Operational Authority that a Subject CA key is compromised; or
- Determination by the Operational Authority that a Subject CA is in violation of this CP, an applicable CPS, or a contractual obligation to a degree that threatens the integrity of the Air Canada PKI.

For Certificates issued by an Air Canada Subordinate CA whose operation involves the use of a cryptographic hardware token, a Subscriber ceasing its relationship with the organisation that sponsored the Certificate shall, prior to departure, surrender to the organisation (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organisation. The token shall be returned to Air Canada and disposed of in accordance with section 6.2.10 promptly upon surrender and shall be protected from malicious use between surrender and such disposition.

If a Subscriber leaves an organisation and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber Certificates associated with the un-retrieved tokens shall be immediately revoked for the reason of key compromise.

4.9.4 Revocation request grace period

There is no revocation grace period. The parties identified in section 4.9.2 must request revocation as soon as they identify the need for revocation.

4.9.5 Time within which CA must process the revocation request

Air Canada Root and PCAs shall process all revocation requests for CA Certificates within six (6) hours of receipt of request.

For Air Canada Subordinate CAs, processing time for Subscriber Certificate revocation

requests shall be as specified below:

Assurance Level	Processing Time for Revocation Requests
basic-software-256 basic-hardware-256	Within thirty-six (36) hours of receipt of request
medium-software-256 medium-hardware-256 medium-device-software-256 medium-device-hardware-256 BEGSS BEGSS-hardware E-EGS E-EGS-hardware	Before next CRL is generated unless request is received within 2 hours of CRL generation

4.9.6 Revocation checking requirement for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL issuance frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

A CA shall ensure that superseded Certificate status information is removed from the PKI Repository upon posting of the latest Certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of Certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements.

Reason	CRL Issuance Frequency
Routine	CAs that are offline and do not issue End-Entity Certificates except for internal operations must issue CRLs at least once every 30 days. At least once every twenty-four (24) hours for all others.

Loss or Compromise of Private Key	Within eighteen (18) hours of request for revocation.
CA Compromise	Immediately, but no later than eighteen (18) hours after notification of such compromise.

CAs that issue routine CRLs less frequently than the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs.

Such CAs shall also be required to notify the other cross-certified PKI domains' Operational Authorities upon Emergency CRL issuance. This requirement shall be included in the respective MOA between Air Canada and other respective PKI domains' responsible organisations.

For off line Root CAs, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 45 days.

For all other CAs, the *nextUpdate* shall be less than or equal to *thisUpdate* plus 48 hours.

4.9.8 Maximum latency for CRLs

The maximum delay between the time a Subscriber Certificate revocation request is received by a CA and the time that this revocation information is available to Relying Parties shall be no greater than twenty-four (24) hours.

The CRL shall be subject to the Repository availability requirements in section 2.1. Care shall be taken by the CA to ensure that the public copy is replaced atomically when it is being updated.

4.9.9 On-line revocation/status checking availability

In addition to CRLs, CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

If a CA supports on-line revocation/status checking, the latency of Certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.

The OCSP availability requirements shall be specified in the relevant Relying Party Agreement.

4.9.10 On-line revocation checking requirements

The Air Canada CAs are not required to operate an OCSP Responder covering the Certificates they issue.

If OCSP is implemented, the Air Canada PKI Repository shall contain and publish a list of all OCSP Responders operated by the Air Canada CAs. In addition, the OCSP service shall comply with the Internet Engineering Task Force (IETF) RFC 6960 to meet security and interoperability requirements.

4.9.11 Other forms of revocation advertisements available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

Any alternative method must meet the following requirements:

- the alternative method must be described in the applicable approved CPS; and
- the alternative method must provide authentication and integrity services commensurate with the Assurance Level of the Certificate being verified.

4.9.12 Special requirements related to key compromise

None beyond those stipulated in section 4.9.7.

4.9.13 Circumstances for suspension

Suspension may be permitted for end-user Certificates issued under all non-device Assurance Levels. Examples of circumstances when suspension may be used are: 1) the discretion of the Certificate issuer; 2) the user's token is temporarily unavailable; 3) authority to use the token has been temporarily suspended; 4) token possession is unknown.

4.9.14 Who can request suspension

A human Subscriber, human supervisor of a human Subscriber, Human Resources (HR) person for the human Subscriber, issuing CA, or RA may request suspension of a Certificate.

4.9.15 Procedure for suspension request

A request to suspend a Certificate shall identify the Certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). The reason code CRL entry extension shall be populated with "certificateHold". The Hold Instruction Code CRL entry extension shall be either absent or contain the OID for idholdinstruction-reject per RFC 5280.

4.9.16 Limits on suspension period

A Certificate may be suspended for up to nine (9) months. The applicable CPS shall describe in detail how this maximum suspension period is enforced. If the Subscriber has not removed the Certificate from hold (suspension) within that period, the Certificate shall be revoked for reason of "Key Compromise".

In order to mitigate the threat of unauthorized person removing the Certificate from hold, the Subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3 or using the Human Subscriber Re-Authentication process described in Section 3.2.3.5. If a Certificate is suspended for a period greater than thirty (30) days, the CA or the RA must verify the need for restoring the credential to the Subscriber. Certificates that have expired or otherwise revoked for other reasons shall not be restored.

4.10 Certificate status services

The Air Canada PKI is not required to support Server-based Certificate Validation Protocol (SCVP).

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate status service.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

Unexpired CA Certificates shall always be revoked at the end of subscription.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Under no circumstances shall a CA or End-Entity signature key be escrowed by a third-party.

For Air Canada CAs that issue encryption Certificates, a Key Recovery Practise Statement (KRPS) shall be developed. The KRPS shall be determined to be compliant with the applicable Key Recovery Policies by the appropriate entity, as required by the appropriate agreements. The Air Canada PMA shall ensure that the PKI operates in compliance with the KRPS.

4.12.2 Session key encapsulation and recovery policy and practices

This CP does not support the recovery of session keys.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The location and construction of the facility housing CA, CSA and CMS equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorised access to the CA, CSA and CMS equipment and records.

Administration Workstations used to administer CA, CSA and/or CMS equipment shall adhere to the requirements identified below except where specifically noted.

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA, CSA and CMS equipment, including any Administration Workstations, shall always be protected from unauthorised access. The physical security requirements pertaining to CA, CSA and CMS equipment, including any Administration Workstations, are:

1. Ensure no unauthorised access to the hardware is permitted
2. Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
3. Ensure manual or electronic monitoring for unauthorised intrusion at all times
4. Ensure an access log is maintained and inspected periodically
5. Provide at least three (3) layers of increasing security such as perimeter, building, and CA room
6. For CAs asserting:
    a. Only Basic Assurance Levels and/or lower: Require controls to physical access and cryptographic modules consistent with those used for commercially sensitive systems
    b. All other Assurance Levels: Require two (2) person physical access control to both the cryptographic module and computer system
7. If a CA shares physical location with a CA of a higher Assurance Level, the CA's physical controls must be as if it were operating at that higher Assurance Level.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorised, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or any removable hardware associated with Administration Workstations.

A security check of the facility housing the CA, CSA, or CMS equipment or Administration

Workstation shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed");
- For off-line CAs and CSA, all equipment other than the PKI Repository is shut down;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorised access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 RA Equipment Physical Access

RA equipment shall be protected from unauthorised access while the RA cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.3 Power and air conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterruptible Power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water exposures

Protection against water exposures shall be in conformance with Air Canada standard data centre procedures. CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 Fire prevention and protection

Fire prevention and protection means shall be in conformance with Air Canada standard data centre procedures.

5.1.6 Media storage

CA media shall be stored so as to protect it from accidental damage (water, fire,

electromagnetic), theft and unauthorised access. Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste disposal

Sensitive waste material shall be disposed of in a secure fashion.

5.1.8 Off-site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored offsite not less than once every seven (7) days, unless the CA is off-line, in which case, it shall be backed up whenever it is activated or every 7 days, whichever is later. At least one (1) full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup data shall be protected with physical and procedural controls commensurate to that of the operational CA. Regular testing of backup data shall be performed to ensure that the data can be restored.

5.2 Procedural Controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles:

- CA System Administrator – authorised to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
- Registration Authority – authorised to request or to approve Certificates or Certificate revocations.
- Audit Administrator – authorised to view and maintain audit logs.
- Operator – authorised to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 CA System Administrator

The CA System Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA;

- Establishing and maintaining CA system accounts;
- Configuring Certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

CA System Administrators shall not issue Certificates to Subscribers.

5.2.1.2 Registration Authority

Personnel designated as Registration Authorities shall be responsible for issuing Certificates; that is:

- Registering new applicants and requesting the issuance of Certificates;
- Verifying the identity of applicants and accuracy of information included in Certificates;
- Entering Subscriber Information, and verifying correctness;
- Approving and executing the issuance of Certificates;
- Requesting, approving and executing the revocation of Certificates;
- Securely communicating requests to, and responses from, the CA; and
- Receiving and distributing Subscriber Certificates.

The RA Role is highly dependent on the Public Key Infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the applicable CPS.

A Trusted Agent must not act as a Registration Authority.

5.2.1.3 Audit Administrator

The Audit Administrator shall be responsible for:

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

5.2.1.4 Operator

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

5.2.1.5 CSA Roles

A CSA shall have at least the following roles.

The CSA administrator shall be responsible for:

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

The CSA Audit Administrator shall be responsible for:

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

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

5.2.1.6 CMS Roles

A CMS shall have at least the following roles which correspond to those listed in section 5.2.1 and are submitted to the same requirements:

The CMS Administrator shall be responsible for:

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

The CMS Audit Administrator shall be responsible for:

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

The CMS Operator shall be responsible for:

- The routine operation of the CMS equipment; and
- Operations such as system backups and recovery or changing recording media.

5.2.1.7 Device Sponsor

A Device Sponsor fills the role of a Subscriber for non-human system components that are named as Public Key Certificate subjects. The Device Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with section 3.2.3.2 and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A Device Sponsor need not be a Trusted role, but should have been issued a credential that is equal to or higher Assurance Level than the credential that they are sponsoring.

5.2.1.8 Trusted Agent

A Trusted Agent is responsible for:

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

A Trusted Agent is NOT a trusted role.

5.2.1.9 Role Sponsor

A Role Sponsor is a Subscriber responsible for the management activities pertaining to the Roles Certificates for which she is the sponsor. The Role Sponsor shall hold an individual Certificate in her own name issued by the same CA at the same or higher assurance level as the Role Certificate being requested for Subscribers. The Role Sponsor need not hold a Role Certificate.

In addition, the Role Sponsor shall be responsible for:

- Authorising individuals for a Role Certificate;
- Recovery of private decryption keys associated with Role Encryption Certificates;
- Revocation of individual Role Certificates;
- Always maintaining a current up-to-date list of individuals who have been issued Role Certificates; and
- Always maintaining a current up-to-date list of individuals who have been provided decryption private keys associated with Role Encryption Certificates.

A Role Sponsor is NOT a trusted role.

5.2.2 Number of persons required per task

Two (2) or more persons shall be required to perform the following tasks:

- CA and CSA Signing key generation;
- CA and CSA Signing key activation; and
- CA and CSA Signing Private Key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1.

Multiparty control shall not be achieved using personnel that serve in the Audit Administrator Role.

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

5.2.3 Identification and authentication for each role

An individual in a Trusted Role shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role.

An individual in a Trusted Role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) access control, where at least one factor is a hardware token shall be used for log in to the Administration Workstation. In addition, the hardware token used must be acceptable for the highest Certificate Policy OID supported by the associated CA. Also see section 6.7 for authentication to the PKI equipment.

All Trusted Roles who operate a CMS shall be allowed access only when authenticated using a method commensurate with medium-hardware-256 requirements.

5.2.4 Roles requiring separation of duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

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

- Individuals who assume a Registration Authority role may not assume an Administrator role;
- Individuals who assume an Audit Administrator role shall not assume any other role; and
- An individual fulfilling the role of Trusted Agent shall not hold any other role within the same CA, except the role of Registration Authority, and shall not perform its own compliance auditor function.
- Under no circumstances shall any of the four roles perform their own compliance auditor function.

No individual fulfilling any of the roles outlined in section 5.2.1 shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

All of the individuals responsible and accountable for the operation of each CA, CSA and CMS shall be identified. The trusted roles of these individuals per section 5.2.1 shall be identified.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation to the extent allowed by law. Personnel appointed to CA trusted roles, CSA trusted roles, CMS trusted roles, and RA role shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the trusted role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance, or had a security clearance revoked for cause;
- Have not been convicted of a serious crime or other offence which affects her suitability for the position; and
- Be appointed in writing by an approving authority.

For CAs issuing Certificates at Medium (or higher) Assurance Levels, each person filling a trusted role shall satisfy the following two requirements:

- One of:
  - The person shall be a citizen of the country where the CA is located; or
  - For CAs located within the European Union, the person shall be a citizen of one of the member states of the European Union; and
- For jurisdictions where obtaining a suitable criminality check or financial verification is not possible, CA/CSA/CMS System Administrators, Audit Administrators, CA/CSA/CMS Operators, and RA Trusted Roles shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) - 22 CFR 120.32.

For RAs, Trusted Agents, and personnel appointed to the trusted roles for the CSAs, in addition to the above, the person may be a citizen of the country where the function is located.

If a given CA shall only be operating at a Basic Assurance Level and/or lower, it is permissible for the trusted roles for that CA not to have any specific clearance or qualification beyond those normally applied to hiring employees of Air Canada, or of those normally stipulated for Air Canada contractors, providing that any such trusted roles do not have any access, privilege or permission on any CA operating at any other Assurance Level higher than the given Basic Assurance Level, and that any component of the Basic Assurance Level CA does not share a logical or physical location with a CA of any other Assurance Level higher than itself.

5.3.2 Background check procedures

All persons filling CA trusted roles, CSA trusted roles, CMS trusted roles, and RA roles shall have completed a background investigation as allowed by applicable national law or regulation. The scope of the background check shall include the following areas covering the past five (5) years and should be refreshed every three (3) years:

- Employment;
- Education (Regardless of the date of award, the highest educational degree shall be verified);
- Place of residence (3 years);
- Law Enforcement; and
- References

Adjudication of the background investigation shall be performed in accordance with the requirements of the appropriate national adjudication authority.

The results of these checks shall not be released except as required in sections 9.3 and 9.4.

For trusted roles filled by employees of Air Canada, an equivalence to this background check may be provided by Air Canada’s Human Resources department.

Individuals that have been issued a valid Restricted Access Identity Card (RAIC) are considered to automatically satisfy this criteria.

Background check procedures shall be described in the CPS.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of a CA, CSA, CMS, or individuals performing Trusted Agent or RA roles shall receive comprehensive training.

Training shall be conducted in the following areas:

- CA/CSA/CMS/RA security principles and mechanisms
- All PKI software versions in use on the CA system, as appropriate to their duties
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining frequency and requirements

Individuals responsible for trusted roles shall be aware of changes in the CA, CSA, or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job rotation frequency and sequence

No Stipulation.

5.3.6 Sanctions for unauthorised actions

The Air Canada PMA shall ensure appropriate administrative and disciplinary actions are taken against personnel who violate this policy in accordance with local labour laws.

5.3.7 Independent contractor requirements

Subcontractor personnel employed to perform functions pertaining to CA, CSA, CMS, or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of section 5.3).

5.3.8 Documentation supplied to personnel

The CA, CSA, and CMS shall make available to its personnel the Certificate Policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties. Documentation shall be maintained identifying all personnel who received training, and the level of training completed.

5.4 Audit Logging Procedures

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

5.4.1 Types of events recorded

All security auditing capabilities of the CA, CSA, CMS, Administration Workstations, and RA operating system and the CA, CSA, CMS, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

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

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

The following events shall be audited[4]:

Auditable Event	CA	CSA	RA	CMS	AW
SECURITY AUDIT					
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X	X
Obtaining a third-party time-stamp	X	X	X	X	X
IDENTITY-PROOFING					
Successful and unsuccessful attempts to assume a role	X	X	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login	X	X	X	X	X

[4] If one or more of the events listed is not applicable to a particular implementation of a PKI component, those non-applicable events need not be audited.

An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X	X
LOCAL DATA ENTRY					
All security-relevant data that is entered in the system	X	X	X	X	X
REMOTE DATA ENTRY					
All security-relevant messages that are received by the system	X	X	X	X	X
DATA EXPORT AND OUTPUT					
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X	X
KEY GENERATION					
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X
PRIVATE KEY LOAD AND STORAGE					
The loading of Component Private Keys	X	X	X	X	X
All access to Certificate subject Private Keys retained within the CA for key recovery purposes	X	N/A	N/A	X	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE					
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X	X
SECRET KEY STORAGE					
The manual entry of secret keys used for authentication	X	X	X	X	X
PRIVATE AND SECRET KEY EXPORT					
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X
CERTIFICATE REGISTRATION					
All Certificate requests	X	N/A	X	X	N/A
CERTIFICATE REVOCATION					
All Certificate revocation requests	X	N/A	X	X	N/A
CERTIFICATE STATUS CHANGE APPROVAL					

The approval or rejection of a Certificate status change request	X	N/A	N/A	X	N/A
PKI COMPONENT CONFIGURATION					
Any security-relevant changes to the configuration of the Component	X	X	X	X	X
ACCOUNT ADMINISTRATION					
Roles and users are added or deleted	X	N/A	N/A	X	X
The access control privileges of a user account or a role are modified	X	N/A	N/A	X	X
CERTIFICATE PROFILE MANAGEMENT					
All changes to the Certificate profile	X	N/A	N/A	X	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT					
All changes to the CSA profile (e.g. OCSP profile)	N/A	X	N/A	N/A	N/A
REVOCATION PROFILE MANAGEMENT					
All changes to the revocation profile	X	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT					
All changes to the Certificate revocation list profile	X	N/A	N/A	N/A	N/A
MISCELLANEOUS					
Appointment of an individual to a Trusted Role	X	X	X	X	X
Designation of personnel for multiparty control	X	N/A	N/A	X	X
Installation of the Operating System	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	N/A
Installation of hardware cryptographic modules	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X
System Start-up	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X
Back up of the internal CA database	X	N/A	N/A	X	N/A
Restoration from back up of the internal CA database	X	N/A	N/A	X	N/A
File manipulation (e.g., creation, renaming, moving)	X	N/A	N/A	N/A	N/A

Posting of any material to a PKI Repository	X	N/A	N/A	N/A	N/A
Access to the internal CA database	X	X	N/A	N/A	N/A
All Certificate compromise notification requests	X	N/A	X	X	N/A
Loading tokens with Certificates	X	N/A	X	X	N/A
Shipment of Tokens	X	N/A	X	X	N/A
Zeroising Tokens	X	N/A	X	X	N/A
Re-key of the Component	X[5]	X	X	X	X
CONFIGURATION CHANGES					
Hardware	X	X	N/A	X	X
Software	X	X	X	X	X
Operating System	X	X	X	X	X
Patches	X	X	N/A	X	X
Security Profiles	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY					
Personnel Access to room housing Component	X	N/A	N/A	X	X
Access to the Component	X	X	N/A	X	X
Known or suspected violations of physical security	X	X	X	X	X
ANOMALIES					
Software error conditions	X	X	X	X	X
Software check integrity failures	X	X	X	X	X
Receipt of improper messages	X	X	X	X	X
Misrouted messages	X	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X	X
Equipment failure	X	N/A	N/A	X	N/A
Electrical power outages	X	N/A	N/A	X	N/A
Uninterruptible Power Supply (UPS) failure	X	N/A	N/A	X	N/A
Obvious and significant network service or access failures	X	N/A	N/A	X	N/A
Violations of Certificate Policy	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X

[5] While this CP prohibits re-key of an Air Canada PKI CA, the audit control should still record any attempt to re-key the CA.

5.4.2 Frequency of processing audit logs

Audit logs shall be reviewed at least once every thirty (30) days, unless the CA is offline, in which case the audit logs shall be reviewed when the system is activated or every 30 days, whichever is later.

Statistically significant sample of security audit data generated by the CA, CSA, CMS, Administration Workstation or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. In addition, the event log of the Administration Workstation shall be reconciled with the event log of the corresponding CA, CMS, or CSA. The Audit Administrator shall explain all significant events in an audit log summary.

Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Actions taken as a result of these reviews shall be documented.

5.4.3 Retention period for audit logs

Audit logs shall be retained onsite for at least sixty (60) days as well as being retained in the manner described in section 5.5. For the CA, CMS, CSA and the Administration Workstations, the Audit Administrator shall be the only person responsible to manage the audit log (e.g., review, backup, rotate, delete, etc.). For RA, a System Administrator other than the RA shall be responsible for managing the audit log.

5.4.4 Protection of audit logs

System configuration and procedures shall be implemented together to ensure that:

- Only authorised people shall have read access to the audit logs. For the CA, CMS, and CSA, the only authorised individual shall be the Audit Administrator. For an RA, the authorised individual shall be a system administrator other than the RA;
- Only authorised people may archive audit logs; and,
- Audit logs shall not be modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up at least once every thirty (30) days,

unless the CA is offline, in which case audit logs and audit summaries shall be backed up when the system is activated or every 30 days, whichever is later. A copy of the audit log shall be sent off-site in accordance with the CPS following review.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the CA, CSA, CMS, or RA. Audit processes shall be invoked at system start-up, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Air Canada PKI PMA shall determine whether to suspend CA operation until the problem is remedied.

5.4.7 Notification to event-causing subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organisation, device, or application that caused the event.

5.4.8 Vulnerability assessments

In addition to the requirements imposed in Section 5.4.2, a vulnerability assessment shall be carried out at least once a year and shall use ISO 27001 as the standard against which PKI operations shall be assessed. Additionally, automated vulnerability assessments are performed at least monthly.

5.5 Records Archival

5.5.1 Types of records archived

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

Once the Administration Workstation logs have been reviewed and reconciled with the corresponding CA, CMS, or CSA logs, they shall be retained for at least one year; further archive of the Administration Workstation logs is not required. However, the reconciliation summary shall be retained for the full archive period prescribed for the CA archive. In addition, events external to the Administration Workstation (e.g. physical access) shall be retained for the full archive period prescribed for the CA archive.

Data To Be Archived	RootCA/CA	CSA	RA	CMS
Certification Practice Statement	X/X	X	X	X
Certificate Policy	X	X	X	X
Contractual obligations	X/X	X	X	X
System and equipment configuration	X/X	X	-	X
Modifications and updates to system or configuration	X/X	X	-	X

Certificate requests	X/X	-	-	X
Revocation requests	X/X	-	-	X
Subscriber identity authentication data as per section 3.2.3	N/A / X	N/A	X	X
Documentation of receipt and acceptance of Certificates, including Subscriber Agreements	X/X	N/A	X	X
Documentation of receipt of Tokens	N/A / X	N/A	X	X
All Certificates issued or published	X/X	N/A	N/A	X
Record of Component CA Re-key	N/A / N/A	X	X	X
All CRLs and CRLs issued and/or published	X/X	N/A	N/A	N/A
All Audit Logs	X/X	X	X	X
Other data or applications to verify archive contents	X/X	X	X	X
Documentation required by compliance auditors	X/X	X	X	X
Compliance Audit Reports	X	X	X	X

5.5.2 Retention period for archive

The retention period for archive data shall depend on the legal and business requirements and is set forth in the respective CPS. However, the archive data must be kept for a minimum retention period of ten (10) years and six (6) months.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of archive

No unauthorised user shall be permitted to write to, modify, or delete the archive. For the CA, CSA, and CMS, the authorised individuals are Audit Administrators. For the RA digital archives, authorised individuals are someone other than the RA. The contents of the archive shall not be released except as determined by the Air Canada PMA for the Air Canada PKI CAs, or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognised agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSA, CMS, or RA) with physical and procedural security controls equivalent or better than those for the component. The archive shall also be adequately protected from environmental threats such as temperature, humidity, radiation, and magnetism.

5.5.4 Archive backup procedures

Adequate and regular backup procedures shall be in place so that in the event of loss or destruction of the primary archives, a complete set of backup copies held in a separate location will be available. The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Procedures detailing how to create, verify, package, transmit and store archive information shall be described in the applicable CPS.

5.6 Key Changeover

To minimise risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected. The key changeover processes shall be described in the applicable CPS.

The following table provides the life times for Certificates and associated Private Keys.

Key	2048 Bits		4096 Bit Keys	
	Private Key	**Certificate**	**Private Key**	**Certificate**
Air Canada Root CAs	20 years	20 years	20 years	20 years
Air Canada Subordinate CAs (tier 1)	5 years	≤10 years	10 years	≤ 13 years[6]
Air Canada Subordinate CAs (tier 2)	3 years	≤ 3 years	Not implemented	Not implemented
Subscriber	3 years	≤ 3 years	Not implemented	Not implemented

[6]For purposes of determining key usage lifetime, it will commence on activation of the key pair.

Identity or Signature				
Subscriber Encryption	n/a	≤ 3 years	Not implemented	Not implemented
Role Identity or Signature	3 years	≤ 3 years	Not implemented	Not implemented
Role Encryption	n/a	≤ 3 years	Not implemented	Not implemented
Code Signing	3 years	≤ 8 years	Not implemented	Not implemented
Server or Device Identity or Signature	3 years	≤ 3 years	Not implemented	Not implemented
Server or Device Encryption	n/a	≤ 3 years	Not implemented	Not implemented
OCSP Responders	3 years	≤ 45 days	Not implemented	Not implemented
SCVP Servers	1 year or 500 000 signatures	≤ 3 years	Not implemented	Not implemented
TSA	≤ 1 year	≤ 20 years	Not implemented	Not implemented
E-EGS LSAPL Signing	5 years	≤ 5 years	Not implemented	Not implemented
E-EGS CSCT Signing	5 years	≤ 5 years	Not implemented	Not implemented
E-EGS Application ID	5 years	≤ 5 years	Not implemented	Not implemented
E-EGS Aircraft Identity ID	7 years	≤ 7 years	Not implemented	Not implemented
E-EGS Aircraft Authentication and Issuing	7 years	≤ 7 years	Not implemented	Not implemented
E-EGS Aircraft Identity and Issuing	7 years	≤ 7 years	Not implemented	Not implemented
BEGSS Aircraft Identity (VPN)	2 years	≤ 2 years	Not implemented	Not implemented
BEGSS EFB Static Identity	5 years	≤ 5 years	Not implemented	Not implemented

No CA shall have a private key whose validity period exceeds 20 years. Cross-Certificates shall not have a validity period exceeding 10 years.

A CA shall not generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. As a consequence, the CA Key Pair shall be changed at the latest at the time of CA Certificate expiration minus Subscriber Certificate validity duration.

Notwithstanding the above table, in all cases the CA private key may be used to sign OCSP Certificates and CRLs until the CA Certificate expires.

5.7 Compromise and Disaster Recovery

Administration Workstations shall be subject to the same incident and compromise handling requirements as the components they administer, including but not limited to compromise investigation, damage assessment, and mitigation planning and implementation.

5.7.1 Incident and compromise handling procedures

A formal disaster recovery plan shall exist for the Air Canada PKI Domain.

If a CA or CSA detects a potential cracking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSA key is suspected of compromise, the procedures outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA or CSA needs to be rebuilt, only some Certificates need to be revoked, and/or the CA or CSA key needs to be declared compromised.

The Air Canada PMA members shall be notified if any of the following cases occur:

- suspected or detected compromise of an Air Canada CA system;
- physical or electronic attempts to penetrate an Air Canada CA system;
- denial of service attacks on an Air Canada CA component;
- any incident preventing an Air Canada CA from issuing a CRL within twenty-four (24) hours of the time specified in the next update field of its currently valid CRL.

The Air Canada PMA members and other domain PKI (who entered a MOA with Air Canada) PMA members shall be notified if any of the following cases occur:

- Revocation of a relevant CA Certificate, such as for a CA cross-certified with the other domain's PKI, is planned;
- any incident preventing such a relevant CA from issuing a CRL within twenty-four (24) hours of the time specified in the next update field of its currently valid CRL.

This will allow the other PKI domains to protect their interests as Relying Parties.

The CA Operational Authority shall re-establish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The CMS shall have documented incident-handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS or CMS keys are compromised, all Certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber Certificates that may have been compromised shall be revoked, and Subscribers shall be notified of

such revocation. The CMS shall be re-established.

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

If a CA or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation shall be re-established as quickly as possible, giving priority to the ability to generate Certificate status information. Before returning to operation make sure the system's integrity has been restored.

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA shall be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties.

If the ability to revoke Certificates is inoperable or damaged, the CA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's revocation capability cannot be established in a reasonable timeframe, the CA shall determine whether to request revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Entity Private Key compromise procedures

If a CA's signature keys are compromised, lost, or suspected to be compromised:

1. All cross certified CAs shall be securely notified at the earliest feasible time (so that entities may issue CRLs revoking any Cross-Certificates issued to the CA);
2. A new CA Key Pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
3. New CA Certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
4. The CA shall request all Subscribers to re-key using the procedures outlined in section 3.3.2; and
5. If the CA is an Air Canada Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The Air Canada PMA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a CSA key is compromised, all Certificates issued to the CSA shall be revoked, if applicable. The CSA will generate a new Key Pair and request new Certificate(s), if applicable. As a CSA operated by the Air Canada PKI may not be a trust anchor, there are no specific requirements regarding trust anchor propagation.

If a CMS key is compromised, all Certificates issued to the CMS shall be revoked. The CMS will generate a new key pair and request new Certificate(s).

If an RA signature keys are compromised, lost, or suspected to be compromised:

1. The RA Certificate shall be immediately revoked;
2. A new RA Key Pair shall be generated in accordance with procedures set forth in the

applicable CPS;

3. A new RA Certificate shall be requested in accordance with the initial registration process set elsewhere in this CP;
4. All Certificate registration requests approved by the RA since the date of the suspected compromise shall be reviewed to determine which ones are legitimate; and
5. For those Certificate requests or approvals that cannot be ascertained as legitimate, the resultant Certificates shall be revoked and their subjects (i.e., Subscribers) shall be notified of revocation.

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster whereby all of a CA's installations are physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its Certificates be revoked. The CA shall follow steps 2 through 5 in section 5.7.3 above.

5.8 CA, CMS, CSA, or RA Termination

In the event of termination of a CA, the CA shall request all Certificates issued to it be revoked.

In the event of a CA termination, the Air Canada PMA shall provide notice to all cross certified CAs prior to the termination. Additionally, in the case of an Air Canada Root CA or Air Canada Subordinate CA termination, cross-certified PKIs will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

A CA, CSA, CMS, and RA shall archive all audit logs and other records prior to termination.

A CA, CSA, CMS, and RA shall destroy all its Private Keys upon termination.

CA, CSA, CMS, and RA archive records shall be transferred to an appropriate authority such as the PMA responsible for the entity.

If an Air Canada Root CA is terminated, that Air Canada Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated Air Canada Root CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Subject Public Keys shall meet the following requirements:

- RSA keys
  - Algorithm OID: rsaEncryption {1.2.840.113549.1.1.1}
  - Parameters: NULL
  - Modulus *m* and public exponent *e* where,
    - *m* is 2048, 3072, or 4096 bits; and
    - $2^{16} < e < 2^{256}$
- Elliptic Curve keys[7]
  - Algorithm OID: ecPublicKey {1.2.840.10045.2.1}
  - Parameters: namedCurve P-256 {1.2.840.10045.3.1.7}
  - Subject Public Key: Uncompressed EC Point

6.1.1 Key pair generation

The following table provides the requirements for Key Pair generation for the various entities.

Entity	FIPS 140-2 Level	Hardware or Software	Key Storage Restricted to the Module on which the Key was Generated
CA	3	Hardware	Yes
CMS	2	Hardware	Yes
RA	2	Hardware	Yes
SCVP Server	3	Hardware	Yes
TSA	3	Hardware	Yes
OCSP Responder	2	Hardware	Yes
Content Signing	2	Hardware	Yes
Card Authentication	2	Hardware	Yes
Code Signing	2	Hardware	Yes
basic-software-256	No requirements	Software	No Requirement

[7] It is assumed that P256 curve is used. If another curve is used, the parameters field shall be populated with the appropriate OID value for that curve.

basic-hardware-256	No requirements	Hardware	No Requirement
medium-software-256 **medium-device-software-256** **BEGSS** **E-EGS**	1	Software	No Requirement
medium-hardware-256 **medium-device-hardware-256** **BEGSS-hardware** **E-EGS-hardware**	2[8]	Hardware	Device or Human Subscriber Encryption: No Requirement Others: Yes

Random numbers for Medium Assurance Level keys shall be generated in FIPS 140-2 Level 2 validated hardware cryptographic modules.

When Private Keys are not generated on the token to be used, originally generated Private Keys shall be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to further act as the key escrow module.

Multi-party control shall be used for CA Key Pair generation, as specified in section 5.2.2.

The CA Key Pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

Activation of the CMS Master Key shall require strong authentication of Trusted Roles. Key diversification operations by the CMS shall also occur on the CMS hardware cryptographic module. The diversification master keys shall only be stored in hardware cryptographic modules that support medium-hardware Assurance Level Certificates. CMS Master Key and diversification master keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage issued cards.

6.1.2 Private Key Delivered to a Subscriber

CAs shall generate their own Key Pair and therefore do not need Private Key delivery.

If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply.

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

[8] For Aircraft Signature, Aircraft Authentication, and Aircraft Encryption Certificates, a formal certification to FIPS 140-2 Level 2 is not required, provided that compliance with the security objectives of FIPS 140-2 Level 2 is demonstrated.

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

The CA or the RA shall maintain a record of the Subscriber acknowledgement of receipt of the token.

6.1.3 Public key delivery to Certificate issuer

Where the Subscriber or RA generates Key Pairs, the Public Key and the Subscriber's identity shall be delivered securely to the CA for Certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the Public Key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the Certificate.

6.1.4 CA Public Key delivery to Relying Parties

The Public Key of a trust anchor shall be provided to the Subscribers acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

- The CA loading a trust anchor onto tokens delivered to Subscribers via secure mechanisms;
- Secure distribution of a trust anchor through secure out-of-band mechanisms;
- Comparison of Certificate hash (fingerprint) against trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); or
- Loading trust anchor from web sites secured with a currently valid Certificate of equal or greater Assurance Level than the Certificate being downloaded and the trust anchor is not in the certification chain for the Web site Certificate.

6.1.5 Key sizes

If the Air Canada PMA determines that the security of a particular algorithm may be compromised, it may require the CAs to revoke the affected Certificates. External PKI domains PMA may require Air Canada CAs to revoke the affected Certificates, according to

the applicable MOA.

All Certificates, CRLs and protocols used by the PKI (e.g., Transport Layer Security (TLS)) shall use the following algorithm suites for the time periods indicated:

Cryptographic Function	Expires before 12/31/2030	Expires after 12/31/2030
Signature	2048 bit RSA per FIPS 186-3 For ECDSA, per FIPS 186-3, 224 bit prime field or 233 bit binary field	3072 bit RSA per FIPS 186-3 For ECDSA, per FIPS 186-3, 256 bit prime field or 283 bit binary field
Hashing	SHA-256	SHA-256
Public Key Encryption	2048 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 224 bit prime field or 233 bit binary field	3072 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 256 bit prime field or 283 bit binary field
Symmetric Encryption	3 Key TDES or AES	AES

Regardless, all CAs shall use 2048 bit RSA, or 224 bit prime field or 233 bit binary field, or stronger.

A CA or OCSP responder whose Certificate is signed using SHA-256 shall not use SHA-1 in its signatures, or rely on signatures using SHA-1.

CSAs shall use the same signature algorithms, key sizes, and hash algorithms as used by the relevant CA to sign its CRL.

6.1.6 Public key parameters generation and quality checking

RSA keys shall be generated in accordance with FIPS 186-3 (except for Certificates at the Basic Assurance Levels). Prime numbers for RSA shall be generated or tested for primality in accordance with FIPS 186-3.

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-3. Curves from FIPS 186-3 shall be used.

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

The use of a specific key is determined by the key usage extension in the X.509 Certificate. For all Certificates, the Certificate Profiles in section 10 specify the allowable values for this extension for different types of Certificates issued by the Air Canada CAs. This includes, but is not limited to, the following examples:

- Certificates to be used for authentication shall only set the digitalSignature bit, except in the case of Certificates used for devices that provide SSL/TLS protocol connections in which case the keyEncipherment bit may also be set;

- Certificates to be used for Digital Signatures shall set the digitalSignature and contentCommitment bits;
- Certificates that have the contentCommitment bit set shall not have the keyEncipherment or keyAgreement bit set;
- Certificates to be used for encryption shall set the keyEncipherment bit;
- Certificates to be used for key agreement shall set the keyAgreement bit;
- CA Certificates shall include cRLSign and keyCertSign bits.

Public keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using Key Management Certificates and require setting both digitalSignature and keyEncipherment bits when RSA is used for the Subject's key pair, or both digitalSignature and keyAgreement when elliptic curves are used for the Subject's key pair.

For Certificates issued to entities other than CAs, the extendedKeyUsage X.509 extension shall always be present and shall not contain the anyExtendedKeyUsage OID {2.5.29.37.0}.

The extended key usage shall meet the requirements stated in section 10.7. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The relevant standards for cryptographic modules are FIPS PUB 140-2, "Security Requirements for Cryptographic Modules". The Air Canada PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Air Canada PMA. Cryptographic modules shall be validated to the FIPS 140-2 level identified in section 6.1, or validated, certified, or verified to requirements published by the Air Canada PMA; Additionally, the Air Canada PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

The table in section 6.1.1 summarises the minimum requirements for cryptographic modules; higher levels may be used. In addition, Private Keys for all Assurance Levels shall not exist outside of their cryptographic modules in plaintext form.

6.2.2 Private Key (n out of m) multi-person control

Use of a CA private signing key or CSA private signing key shall require action by at least two (2) persons.

6.2.3 Private Key escrow

Under no circumstances shall a third party escrow any Signature key.

End-Entity Private Keys used solely for decryption shall be escrowed prior to the generation

of the corresponding Certificates, with the exception of decryption Private Keys associated with aircraft and/or aircraft equipment encryption Certificates, which do not need to be escrowed.

6.2.4 Private Key backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as that used to generate and protect the original signature key. A single backup copy of the signature key shall be stored at or near the CA location.

A second backup copy shall be kept at the CA backup location.

Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of section 5.2.2.

6.2.4.2 Backup of Subscriber Private Signature Key

Human Subscriber private signature keys whose corresponding Public Key is contained in a Certificate which does not assert any hardware Assurance Levels may be backed up or copied but must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

Human Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting a hardware Assurance Level for human Subscriber shall not be backed up or copied.

Device private signature keys whose corresponding Public Key is contained in a Certificate asserting Medium-device-hardware-256 or E-EGS-hardware Assurance Levels shall not be backed up or copied, with the exception of the Device signature keys used for specific remote signing applications (e.g., CSCT, TRAX) that shall be backed up under the same controls as used to generate and protect the original signature key.

For all other Device Subscriber Assurance Levels, the Private Key may be backed up or copied but must be held in the control of the device's human sponsor. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.4.3 CSA Private Key Backup

If backed up, the CSA private signature keys shall be backed up under the same multi-person control as used to generate the CSA private signature keys, and shall be accounted for and protected in the same manner as the original. A single backup copy of the CSA private signature key may be stored at or near the CSA location. A second backup copy may be kept at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.5 Private Key archival

Private signature keys shall not be archived.

For some applications (e.g., protected aircraft to ground communications), the device key

may be archived by the CA, upon crypto-period expiration and/or key replacement, to support recovery of encrypted messages, as necessary to comply with regulatory requirements regarding data retention. Such archives shall be described in an Air Canada PKI Key Recovery Practise Statement (KRPS).

6.2.6 Private Key transfer into or from a cryptographic module

CA, CSA and CMS Private Keys shall be generated by and remain in an approved cryptographic module.

The CA, CSA and CMS Private Keys may be backed up in accordance with section 6.2.4.1.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key storage on cryptographic module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module. Private Keys must be stored on a cryptographic module at least as strong as that referenced in section 6.1.1 for that key's generation.

6.2.8 Method of activating Private Key

The user of a cryptographic module must be authenticated to the cryptographic module before the activation of any Private Key(s), except as indicated below. Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For Certificates issued under any of the medium-device policies, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9 Method of deactivating Private Key

The cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorised access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA, CSA and CMS hardware cryptographic modules shall be removed and stored in a secure container when not in use. Hardware cryptographic modules used by RAs shall be removed and either stored in a secure container or kept on the person of the RA when not in use.

6.2.10 Method of destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software cryptographic

modules, this can be done by overwriting the data. For hardware cryptographic modules, this usually requires executing a "zeroise" command. Physical destruction of hardware is generally not required. For CA, RA, CMS, and CSA private signature keys, the keys shall be destroyed by individuals in Trusted Roles.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The Public Key is archived as part of the Certificate archival.

6.3.2 Certificate operational periods and Key Pair usage periods

See section 5.6.

6.3.3 Organizational Code-Signing Certificate, or Role-Based Aircraft Code-Signing Keys

For a Code-Signing Certificate issued to a group as a whole, the group's manager must keep a log stating possession of the Private Key, including the name of the individual to whom the Private Key was entrusted, and the time and date it was entrusted to them. For Role-based Code Signing Certificates where the Private Keys are used to sign Aircraft software parts, the Role Sponsor shall keep a log stating to whom such Role Certificates were issued. This log must be kept for a minimum of thirty (30) years. The Entity operating the CA shall ensure that there is a binding between the Role Certificate and the individual Subscriber to whom it is being issued. Such binding shall be commensurate with the Assurance Level of the Certificates being issued. The Subscriber and/or Subscriber's employer are responsible to ensure that the individual in possession of the Private Key corresponding to a Certificate of either type complies with this CP. Moreover, log information maintained by the Subscriber and Subscriber's employer may be audited by the CA or RA at any time.

6.4 Activation Data

6.4.1 Activation data generation and installation

For Certificates issued under any of the medium-device policies, private keys may be activated without entry of activation data.

For other assurance levels, the activation data used to unlock Private Keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the crypto module used to store the keys. Subscriber activation data may be user selected. For CAs, it shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated

cryptographic module.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

CAs, CSAs, and RAs shall change the activation data whenever the token is re-keyed or returned from maintenance.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSA, CMS, Administration Workstations, and RA shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Provide domain isolation for process
- Provide self-protection for the operating system
- Require self-test security related CA services (e.g., check the integrity of the audit logs)
- Support recovery from key or system failure

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The CA-computer system shall be configured with the minimum number of required

accounts, and network services, and no remote login functionality.

The Air Canada Root CAs shall be operated offline with no network connections installed.

6.5.2 Computer security rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The System Development Controls for the CA, CSA, and CMS are as follows:

- Shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software developed shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications, hardware devices, network connections, or component software installed which are not parts of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations shall be obtained from sources authorised by local policy. CA, CSA, CMS, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security management controls

The configuration of the CA, CSA and CMS systems as well as any modifications and upgrades shall be documented and controlled.

There shall be a mechanism for detecting unauthorised modification to the CA, CSA and CMS software or configuration.

A formal configuration management methodology shall be used for installation and on-going maintenance of the CA and CMS systems. The CA and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

All Administration Workstations shall be dedicated to remote administration and shall be protected while at rest. In particular, they shall not be used as personal workstations. The Administration Workstations shall be maintained at the same level as the equipment they access (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this workstation as well).

In addition, only applications required to perform the organisation's mission shall be loaded on the RA workstation, and all such software shall be obtained from sources authorised by local policy.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network Security Controls

The Air Canada Root CAs and their internal PKI Repositories shall be off-line.

Air Canada Sub Signing CAs, CSAs, CMSes, Administration Workstations, and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

If the Administration Workstation is located outside the security perimeter of the CA, CMS, and CSA, it shall access the PKI equipment using site-to-site VPN. The VPN shall use FIPS-approved cryptography commensurate with the cryptographic strength of Certificates issued by the PKI being administered. The VPN shall be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret-based, the shared secret shall be changed at least annually, shall be randomly generated, and shall have entropy commensurate with the cryptographic strength of Certificates issued by the PKI being administered. Alternatively, when the Administration Workstation is located inside the security perimeter of the CA, CMS, and CSA, and protected by the boundary controls of the PKI equipment, appropriate techniques shall be used for mutual authentication of the PKI components and mutual authentication of traffic flowing among them.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Remote access shall be mediated by a bastion host or "jump point" (i.e. a machine that presents a limited interface for interaction). All network activity to the PKI components (e.g. CA, CMS, and/or CSA) shall be initiated from the bastion host. The bastion host is considered part of the CA, CMS, and/or CSA and shall meet the security requirements for these components. A remote workstation or user shall perform mutual authentication with the bastion host using strong authentication (e.g., PKI credential) commensurate with the cryptographic strength of Certificates issued by the PKI being administered. Cryptographic material derived from the authentication shall be used to protect the communication with the bastion host. In addition, the user shall authenticate to the PKI component being administered via the bastion host. In other words, authentication to the bastion host does not alleviate the need to authenticate to the PKI component(s) being administered.

Remote administration shall be designed such that there are positive controls to meet the two-person control requirements specified in this CP and in the appropriate KRP. In addition, the remote administration shall be designed such that there are positive controls to meet the requirement for the Audit Administrator to control the event logs. Remote administration shall continue to fully enforce the integrity, source authentication and destination authentication, as applicable for administrative functions such as configuration, patch management, and monitoring.

RA equipment shall, at a minimum, be protected by a local firewall and malware protection. Additionally, all access by the RA equipment to the CA shall be via a protected and authenticated channel using cryptography commensurate with the level of the credentials being managed by that RA.

6.8 Time-Stamping

All CA, CSA, and CMS components shall regularly synchronise with a time service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSA responses

Asserted times shall be accurate to within three (3) minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4.1.

7 Certificate, CRL, and OCSP Profiles

7.1 CERTIFICATE PROFILE

7.1.1 Version number(s)

The CAs shall issue X.509 v3 Certificates (populate version field with integer "2").

7.1.2 Certificate extensions

Air Canada CAs' critical private extensions shall be interoperable in their intended community of use.

Air Canada Subordinate CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains the Certificate formats.

7.1.3 Algorithm object identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
Ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}

Certificates under this CP shall use the following OID for identifying the subject Public Key information:

rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-key-type(2) 1}

7.1.4 Name forms

The subject and issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC 5280. Subject and Issuer fields shall include attributes as detailed in the tables below

Subject Name Form for CAs

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	CN	0…1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0…N	As needed

	Recommended	OU	0…1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc"
	Optional	ST	0…1	State or Province Name, e.g., "ST=California"
	Required	C	1	Country name, e.g., "C=US"
2	Required	CN	0…1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	"Certification Authorities" or similar text
	Optional	O	0…1	Issuer name, e.g., "O=XYZ Inc"
	Optional	ST	0…1	State or Province name, e.g., "ST=California"
	Optional	C	0…1	Country name, e.g., "C=US"
	Required	DC	1	Domain name, e.g., "DC=xyzinc"
	Required	DC	1…N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc.
3	Required	CN	1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Required	dnQualifier	1	DN Qualifier
	Required	description	1	Airplane
	Required	x500UniqueIdentifier	1	Unique Identifier
	Required	OU	1	Aircraft or AircraftCA
	Required	OU	1	ACM
	Required	O	1	Air Canada
	Required	C	1	CA

Subject Name Form (Other Subscribers)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content	1…N	Additional naming attributes for uniquely identifying the subject including common name,

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
		description		serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate of the Issuer
	Required	C	1	Country name, e.g., "C=US" exactly as it appears in the CA Certificate of the Issuer
2	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	DC	1	Domain name, e.g., "DC=xyzinc" exactly as it appears in the CA Certificate of the Issuer
	Required	DC	1…N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as it appears in the CA Certificate of the Issuer

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

Aircraft Identification shall be an identifier registered in an aerospace industry-recognised registry and verifiable by the CA (e.g.: aircraft registration / tail number).

Aircraft Equipment Identification shall be an identifier registered in an aerospace industry-recognised registry and verifiable by the CA (e.g.: equipment registration number).

7.1.5 Name constraints

The CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in section 10 subject to the requirements above.

The Air Canada CAs shall not obscure a Subscriber Subject name. Issuer names shall not be obscured. Air Canada CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6 Certificate Policy object identifier

CA and Subscriber Certificates issued under this CP shall assert one or more of the Certificate Policy OIDs listed in section 1.2 of this document.

A CA Certificate shall contain the policy OIDs of all policies under which it issues

Certificates.

Certificates issued under the BEGSS Trusted Root shall only contain the BEGSS policy OIDs.

Certificates issued under the E-EGS Trusted Root shall only contain the E-EGS policy OIDs.

For non-CA Certificates, the Certificate asserting a policy OID shall also assert all lower assurance policy OIDs, within the restrictions outlined below. (Refer to Figure 2 in section 1.2 for the Assurance Level hierarchy.)

Thus, for example, a CA issuing Certificates at all Assurance Levels shall assert the following OIDs in Certificates it issues:

ASSURANCE LEVEL	OIDS ASSERTED
basic-software-256	1.3.6.1.4.1.49507.1.1.9
basic-hardware-256	1.3.6.1.4.1.49507.1.1.10 1.3.6.1.4.1.49507.1.1.9
medium-software-256	1.3.6.1.4.1.49507.1.1.11 1.3.6.1.4.1.49507.1.1.9
medium-hardware-256	1.3.6.1.4.1.49507.1.1.12 1.3.6.1.4.1.49507.1.1.11 1.3.6.1.4.1.49507.1.1.10 1.3.6.1.4.1.49507.1.1.9
medium-device-software-256	1.3.6.1.4.1.49507.1.1.13
medium-device-hardware-256	1.3.6.1.4.1.49507.1.1.14 1.3.6.1.4.1.49507.1.1.13
BEGSS	1.3.6.1.4.1.49507.1.2.1
BEGSS-hardware	1.3.6.1.4.1.49507.1.2.2 1.3.6.1.4.1.49507.1.2.1
E-EGS	1.3.6.1.4.1.49507.1.3.1
E-EGS-hardware	1.3.6.1.4.1.49507.1.3.2 1.3.6.1.4.1.49507.1.3.1

7.1.7 Usage of Policy Constraints extension

The Air Canada PKI policy domain shall follow the Certificate formats described in this CP, since inhibiting policy mapping may limit interoperability.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, CP and CPS pointers.

7.1.9 Processing semantics for the critical Certificate Policies extension

Processing semantics for the critical Certificate Policy extension shall conform to X.509 certification path processing rules. Where such rules conflict with IETF RFC 5280, RFC 5280 shall be followed.

7.2 CRL PROFILE

7.2.1 Version number(s)

CAs shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL and CRL entry extensions

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

Section 10 contains the CRL formats.

7.3 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 6960. Section 10 contains the OCSP request and response formats.

7.3.1 Version number(s)

The version number for request and responses shall be v1.

7.3.2 OCSP extensions

Responses shall support the nonce extension.

8 Compliance Audit and Other Assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the contracts (including MOA) with cross-certified CAs are being implemented and enforced.

8.1 Frequency or circumstances of assessment

The Air Canada PKI shall be subject to a periodic compliance audit at least once every 2 years.

The OA has the right to require unscheduled compliance inspections of subordinate CA, CSA, CMS, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS.

The Air Canada PMA has the right to require unscheduled compliance audits of all entities in the Air Canada PKI. The Air Canada PMA shall state the reason for any unscheduled compliance audit. This compliance audit allows the Air Canada PMA to authorise or not (regarding the audit results) the Air Canada CAs to operate under this CP.

In the context of cross-certification, audits shall be requested as stated in the respective contracts and/or MOA.

8.2 Identity and qualifications of assessor

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with the requirements of this CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

8.3 Assessor’s relationship to assessed entity

The compliance auditor shall be a firm, which is independent from Air Canada and its affiliated companies, as well as subcontractors operating the Air Canada PKI. The Air Canada PMA shall determine whether a compliance auditor meets this requirement and all applicable MOAs.

8.4 Topics covered by assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP, the applicable CPSes, and the applicable MOAs.

The compliance audit must include an assessment of the applicable CPS against this CP, to determine that the CPS adequately addresses and implements the requirements of the CP.

8.5 Actions taken as a result of deficiency

The Air Canada PMA or cross certified PKI PMAs may determine that a CA is not complying with its obligations set forth in this CP or the respective contracts (including MOAs) with cross-certified PKIs.

When such a determination is made, the PMA may suspend operation, may revoke the CA, or take other actions as appropriate. The respective CPS shall provide the appropriate

procedures.

When the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, any contract with cross-certified PKIs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Air Canada PMA of the discrepancy;
- The Air Canada PMA shall notify any affected cross-certified external PKI domains' PMAs promptly; and
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the respective contracts, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy and how quickly it can be corrected, the PMA may decide to halt temporarily operation of the CA, to revoke a Certificate issued by the CA, or take other actions it deems appropriate. The PMA shall develop procedures for making and implementing such determinations.

8.6 Communication of results

An Audit Compliance Report package, including identification of corrective measures taken or being taken by the component, shall be provided to the PMA as set forth in section 8.1. This package shall be prepared in accordance with the "Compliance Audit Reference Documents" and must include an assertion from the PMA that all PKI components have been audited – including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

PRACTICE NOTE:

The different components of the Infrastructure may be audited separately. In these cases, the Compliance Audit Package will contain multiple audit reports, one for each separately audited component

8.7 Retention of Audit report

Results of all Audits, as well as the data used to generate these results must be kept for a minimum of twenty (20) years or as further required by applicable law or industry regulation.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Air Canada is entitled to charge end-user Subscribers for the issuance, management, modification, re-key, and renewal of Certificates provided by the Air Canada PKI.

9.1.2 Certificate access fees

The management of Air Canada shall decide on any fees related to the Air Canada PKI services.

There shall be no fee associated with Relying Party access to Certificates in the Air Canada PKI Directory.

9.1.3 Revocation or status information access fees

The management of Air Canada shall decide on any fees related to the Air Canada PKI services.

There shall be no fee associated with Relying Party access to revocation or status information.

9.1.4 Fees for other services

The management of Air Canada shall decide on any fees related to the Air Canada PKI services.

9.1.5 Refund policy

Air Canada offers no refunds on issued Certificates.

9.2 Financial responsibility

9.2.1 Insurance coverage

Air Canada shall maintain reasonable levels of insurance coverage as required by applicable laws.

9.2.2 Other assets

Air Canada shall maintain sufficient financial resources to maintain operations and fulfil duties.

9.2.3 Insurance or warranty coverage for End-Entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of Confidential Information

Business or corporate information held by a CA or an RA which does not appear in Certificates or in public directories is considered confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Any information made public in a certificate is deemed not confidential. In that respect, Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or confidential.

9.3.3 Responsibility to Protect Confidential Information

Each CA shall maintain the confidentiality of confidential business information that is clearly marked or labelled as confidential or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

Confidential business or corporate information shall not be disclosed by the CA or RA, unless required by valid law or court order.

9.4 Privacy of personal information

For the purposes of the PKI related services, the Air Canada PKI collects, stores, processes and discloses personally identifiable information in accordance with applicable laws and regulations, specifically PIPEDA, the EU Data Protection Directive 95/46/EC and the Air Canada Corporate Data Privacy Policy.

9.4.1 Privacy Plan

The collection and storage of Personally Identifiable Information shall be limited to the minimum necessary to validate the identity of the Subscriber. Personally Identifiable Information collected for identity proofing purposes shall not be used for any other purpose. This may include attributes that correlate identity evidence to authoritative sources. Personally Identifiable Information collected for identity proofing purposes shall not be used for any other purpose.

Subscribers and End-Entities must be given access and the ability to correct or modify their personal or organization information upon appropriate request to the issuing CA. Such information must be provided only after taking proper steps to authenticate the identity of the requesting party.

9.4.2 Information Treated as Private

Personally Identifiable Information held by a CA or an RA which does not appear in Certificates or in public directories is considered private and shall not be disclosed by the CA or RA.

9.4.3 Information Not Deemed Private

Subscribers acknowledge that any information included in a certificate is deemed as not private. In that respect, Certificates, OCSP responses, CRLs and Personally Identifiable Information appearing in them and in public directories are not considered private.

9.4.4 Responsibility to Protect Private Information

All information collected as part of the identity proofing process shall be protected to ensure confidentiality and integrity. In the event that the PKI activities are terminated, the PKI shall be responsible for disposing of or destroying sensitive information, including Personally Identifiable Information, in a secure manner, and maintaining its protection from unauthorized access until destruction.

Personally Identifiable Information shall not be disclosed by the CA or RA, unless required by valid law or court order.

9.4.5 Notice and Consent to Use Private Information

The RA shall provide explicit notice to the Subscriber regarding the purpose for collecting and maintaining a record of the Personally Identifiable Information necessary for identity proofing and the consequences for not providing such Personally Identifiable Information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA, CMS, and RA shall protect all Subscriber Personally Identifiable Information from unauthorized disclosure. The contents of the archives maintained by the CA shall not be released except as required by law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual property rights

The Air Canada PKI owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

The Air Canada PKI Operational Authority shall not violate intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

Air Canada CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

Air Canada grants permission to reproduce and distribute its Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to a Relying Party Agreement with the relevant CA. Air Canada shall grant permission to use revocation information to perform Relying Party functions, subject to applicable contractual agreements.

The Subscriber, who has a Certificate delivered by Air Canada PKI, retains all intellectual

rights it has on the information contained in the Certificate delivered by an Air Canada CA (subject name). An external CA, which cross-certifies with the Air Canada PKI, retains all intellectual rights it owns on the information contained in the CA Certificate delivered by Air Canada PCAs (CA distinguished name, Public Key, policy OID…)

9.5.2 Property Rights in this CP and related CPSes

Air Canada asserts that it owns and/or has licensed the Intellectual Property Rights to this CP and related CPS. Furthermore, Air Canada reserves all Intellectual Property Rights in this CP and related CPSes to be granted to Licensors at its discretion in conjunction with all applicable agreements and licenses.

9.5.3 Property Rights in Names

The Certificates may contain copyrighted material, trademarks and other proprietary information, and no commercial exploitation or unauthorised use of the material or information in or via the Certificates is permitted, except as may be provided in this CP or in any applicable agreement. In the event of any permitted use or copying of trademarks and/or copyrighted material, no deletions or changes in proprietary notices shall be made without written authorisation from the owner.

9.5.4 Property Rights in Keys

Key pairs corresponding to Certificates of cross-certified CAs and Subscribers are the property of the cross-certified CAs and Subscribers that are the respective subjects of these Certificates, subject to the rights of Subscribers regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these Key Pairs. Notwithstanding the foregoing, Air Canada Root CAs' root Public Keys and the root Certificates containing them, including all PCA Public Keys and self-signed Certificates, are the property of Air Canada.

9.6 Representations and warranties

The Air Canada PKI provides its services in accordance with applicable laws and regulations.

Additional representations and warranties of Air Canada PKI and contractual partners are contained in the respective contractual documents. This includes agreement on responsibility for export compliance.

9.6.1 CA representations and warranties

9.6.1.1 The Air Canada Root CAs

The Air Canada OA represents that, to its knowledge:

- Their Certificates meet all material requirements of this CP, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

The applicable agreements may include additional representations and warranties.

9.6.1.2 Air Canada Subordinate or Cross-Certified CAs

Signing Subordinate and Cross-Certified CAs represent and warrant that:

- There are no material misrepresentations of fact in the Cross-Certificates known to or originating from the entity approving the Cross-Certification Applications or issuing the Cross-Certificates,
- There are no errors in the information in the Cross-Certificate that were introduced by the entity approving the Cross-Certification Application or issuing the Cross-Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their CA signing key is protected and that no unauthorised person has ever had access to the Private Key,
- All representations made by the Subordinate CA or Cross-Certified CA in the applicable agreements are true and accurate, and
- All information supplied by the Subscriber in connection with, and/or contained in the Certificate has been duly verified,
- The Certificate is being used exclusively for authorised purposes, consistent with this and any other applicable CP or CPS.

9.6.2 Subscriber representations and warranties

An Air Canada CA shall require the Subscribers to sign a document containing the requirements the Subscriber shall meet respecting protection of the Private Key and use of the Certificate before being issued the Certificate. Subscribers shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- The information in the Subscriber's certificate is accurate.
- Protect their Private Keys at all times and prevent them from unauthorised access in accordance with this policy, as stipulated in their Subscriber Agreement.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their Private Keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CP.
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates, as set forth in this CP and the Subscriber Agreement.
- Use Certificates provided by the Air Canada CAs only for authorised and legal purposes in accordance with this CP.
- Comply with all export laws and regulations for dual usage goods as may be applicable, as relates to the usage and transport of keys, Certificates and algorithms mandated by this CP.
- Cease to use Air Canada Certificates if they become invalid and remove them from any applications and/or devices they have been installed on.

Device Sponsors (as described in section 5.2.1.4) shall assume the obligations of

Subscribers for the Certificates associated with their components.

9.6.3 Relying Party representations and warranties

Parties who rely upon the Certificates issued under a policy defined in this document shall:

- use the Certificate for the purpose for which it was issued, as indicated in the Certificate information (e.g., the key usage extension);
- check each Certificate for validity, using procedures described in section 6 of [RFC 5280], prior to reliance;
- establish trust in the CA who issued a Certificate by verifying the Certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

9.6.4 Representations and warranties of other participants

The Air Canada PMA shall insure that Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the Certificate information posting and retrieval stipulations of this CP; and
- provide access control mechanisms sufficient to protect repository information as described in section 2.4.

An OCSP Responder that has been issued an Air Canada PKI CA Certificate shall conform to the stipulations of this document including operating under a CPS that has been approved by the Air Canada PMA. Such OCSP Responders which are found to have acted in a manner inconsistent with these obligations are subject to action as described in section 8.5.

Affiliated Organisations shall authorise the affiliation of Subscribers with that Organisation, and shall inform the CA of any severance of affiliation with any current Subscriber.

9.7 Disclaimers of warranties

To the extent permitted by applicable law, Policy Mapping Agreements, Cross-Certificates Agreements, Memorandums of Agreement, and any other related agreements may contain disclaimers of all warranties (other than any express warranties contained in such agreements or set forth in this CP).

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN AIR CANADA AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY AIR CANADA AND THE AIR CANADA PKI ARE PROVIDED "AS IS", AND AIR CANADA, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF

INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY AIR CANADA CERTIFICATES, ANY SERVICES PROVIDED BY AIR CANADA, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 Limitations of liability

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreement, subject to the applicable law governing the relationship between the parties.

The liability (and/or limitation thereof) of Air Canada to other PKI domains' CAs to which Air Canada CAs issue Certificates shall be set forth in the applicable agreements.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements between the applicable CA and the Relying Party.

FOR BASIC ASSURANCE CERTIFICATES, ALL LIABILITY ARISING OUT OF OR RELATING TO IMPROPER ACTIONS BY THE AIR CANADA CA ARE DISCLAIMED, AS PERMITTED BY LAW.

FOR ALL OTHER CERTIFICATES OF OTHER ASSURANCE LEVELS, THE TOTAL, AGGREGATE LIABILITY OF EACH AIR CANADA CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE AIR CANADA CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND THE TOTAL LIABILITY OF AIR CANADA SHALL NOT EXCEED A MAXIMUM OF ONE MILLION DOLLARS ($1 MILLION USD) IN AGGREGATE.

9.9 Indemnities

9.9.1 Indemnification by Customer CAs

To the extent permitted by applicable law, other PKI domains CAs issued Certificates by Air Canada agree to indemnify and hold Air Canada harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Air Canada may incur as a result of:

- Falsehood or misrepresentation of fact by the other PKI domains CA in the applicable contractual agreements; or
- Failure by the other PKI domains CA to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party; or
- The other PKI domains CA's failure to protect the other PKI domains CA Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the other PKI domains CA Private Key; or
- The other PKI domains CA's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold Air Canada harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Air Canada may incur as a result of:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Any applicable contractual agreement with Air Canada may include additional indemnity obligations.

9.9.3 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold Air Canada harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Air Canada may incur as a result of:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application; or
- Fraudulent or negligent use of Certificates by the Subscriber; or
- Unauthorised use of the Certificates by Subscribers including use of Certificates beyond the prescribed use defined by this CP; or
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party; or
- The Subscriber's failure to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's Private Key; or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

This indemnification clause shall not be applicable for Air Canada Employees.

9.10 Term and termination

9.10.1 Term

This CP becomes effective upon its execution by the Air Canada PMA and publication in the appropriate directory (as defined in section 2). Amendments to this CP shall become

effective upon execution by the Air Canada PMA and publication in the appropriate Repository (as defined in section 2).

9.10.2 Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version.

Air Canada may decide to terminate this CP at any time. All entities shall be notified 6 (six) months prior to the effective termination of this CP.

9.10.3 Effect of termination and survival

Upon termination of this CP, CAs cross-certified with or subordinate to Air Canada PKI CAs are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. The following sections of this CP shall survive any termination or expiration of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

9.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, Air Canada PKI OA shall use commercially reasonable methods to communicate with cross certified CAs, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for amendment

The Air Canada PMA shall review this CP and the respective CPSes at least once every year. Additional reviews may be enacted at any time at the discretion of the Air Canada PMA.

If the Air Canada PMA wishes to recommend amendments or corrections to the CP or CPS, such modifications shall be circulated to appropriate parties identified by the Air Canada PMA. Comments from such parties will be collected and considered by the Air Canada PMA in a fashion prescribed by the Air Canada PMA.

Following approval by the Air Canada PMA, public notification of amendments shall be made.

Notwithstanding the foregoing, if the Air Canada PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of Air Canada, the Air Canada PMA shall be entitled to make such amendments effective immediately upon publication in the Repository without having to circulate the amendments prior to their adoption.

9.12.2 Notification mechanism and period

Errors, updates and anticipated changes to the CP and CPS resulting from reviews are provided to the Air Canada PMA by the OA Administrator. In addition, the OA Administrator shall communicate changes to every affected entity, including cross-certified PKIs, via a

designated point of contact, including a description of the change.

This CP and any subsequent changes shall be made publicly available within seven (7) days of approval by the Air Canada PMA.

The most up to date copy of this CP can be found at:

https://pub.ac.carillon.ca/CertificatePolicy.pdf

9.12.3 Circumstances under which OID must be changed

Certificate Policy OIDs shall be changed if the Air Canada PMA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute resolution provisions

9.13.1 Disputes among the Air Canada PMA/OA and Third Parties

Provisions for resolving disputes between the Air Canada PKI PMA/OA and contractually linked entities shall be set forth in the applicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

In case of any dispute or disagreement between two or more participants arising out of or related to this CP, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one disputing party to the other. If the dispute is not successfully resolved by negotiation between the entities or the parties within sixty (60) days following the date of such notice, it shall be settled by final and binding arbitration before a single arbitrator knowledgeable in the information technology industry in accordance with the then existing Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC). The place of arbitration shall be defined in the relevant agreement between contracting parties. In the absence of such agreement, the place of arbitration shall be Montreal, Quebec, Canada.

This provision does not limit the right of a party to obtain other recourse and relief under any applicable law for disputes or disagreements that do not arise out of or which are not related to this CP.

9.14 Governing law

Subject to any limits appearing in applicable law, the criminal laws of Canada and the civil laws of the Province of Quebec, shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Canada or Quebec.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with applicable law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

Parties agree to conform to applicable laws and regulations.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulations.

9.16.2 Assignment

Except as otherwise provided under the applicable agreements, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party, except that Air Canada may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Failure or delay at any time to enforce any right hereunder shall not constitute a waiver of such right or affect the validity of the CP or any part thereof, nor shall it prejudice the rights to enforce such right at a subsequent time.

9.16.5 Force Majeure

Air Canada shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

AIR CANADA HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD-PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO AIR CANADA.

9.17 Other provisions

No stipulation.

10 Certificate, CRL, and OCSP Formats

This section contains the formats for the various PKI objects such as Certificates, CRLs, and OCSP requests and responses. The section only contains Certificate profiles based on RSA. For algorithm identifiers, parameter encoding, Public Key encoding, and signature encoding for ECDSA and ECDH, IETF RFC 3279 shall be used.

Certificates and CRLs issued under a policy OID of this CP may contain extensions not listed in the profiles in this section only upon Air Canada PMA approval.

First entries in the caIssuers field of the AIA extension and CRL DP shall point to a resource that is publicly available using HTTP. If LDAP pointers are used, they shall appear only after the HTTP pointers.

For attribute values other than dc and e-mail address: All CA Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as printable string. All Subscriber DN portions that name constraints apply to, shall be encoded as printable string. Other portions of the Subscriber DN shall be encoded as printable string if possible. If a portion cannot be encoded as printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

All dc and email address attribute values shall be encoded as IA5 string.

CAs may issue partitioned CRLs as long as the CRLs are not indirect CRLs, are not partitioned by reason code, and CRL DP and Issuing Distribution Point do not assert name relative to issuer. If the Entity PKI provides OCSP services for a CA, that CA must also issue a full and complete CRL (i.e., a CRL without Issuing Distribution Point extension) for use by the OCSP Responder.

The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain one or more HTTP (i.e., of the form http://…) URI(s) and may be followed by one or more LDAP (i.e., of the form ldap://…) URI(s). The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativeToCRLIssuer).

Global Unique Identifier (GUID) used in Certificates shall conform to [RFC 4122] requirement. Since GUID is associated with a card, the same GUID shall be asserted as UUID in all applicable Certificates and in all applicable other signed objects on the card.

10.1 PKI component Certificates

10.1.1 Air Canada PCA → CBCA G2 Certificate

FIELD	**VALUE**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	cn=CertiPath Bridge CA – G2, ou=Certification Authorities, o=CertiPath LLC, c=US
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
EXTENSION	**VALUE**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; Applicable certificate policies from Section 1.2
Policy Mapping	c=no; Applicable certificate policy mappings
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	Not present
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to PCA, may be followed by LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

10.1.2 Air Canada Self-Signed Roots (Trust Anchors)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, contentCommitment
Basic Constraints	c=yes; cA=True; path length constraint absent

10.1.3 Air Canada Subordinate CAs (Enterprise)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints	c=yes; cA=True; pathLength = 0;
Name Constraints	c=no; PERMITTED: at least DIRNAME equal to the last two RDN values of the Subject DN
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA
CRL Distribution Points	c = no;

10.1.4 Air Canada Intermediate CAs (BEGSS and E-EGS)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; As per section 7.1.6, only BEGSS or E-EGS
Basic Constraints	c=yes; cA=True; pathLength = 1;
Name Constraints	c=no; PERMITTED: at least DIRNAME equal to the last two RDN values of the Subject DN
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA
CRL Distribution Points	c = no;

10.1.5 Air Canada Subordinate CAs (BEGSS and E-EGS)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints	c=yes; cA=True; path length constraint is absent
Name Constraints	c=no; PERMITTED: at least DIRNAME equal to the last two RDN values of the Subject DN
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA
CRL Distribution Points	c = no;
Subject Alternative Name	c=no; aircraft URI (optional)

10.1.6 OCSP Responder Certificate

The following table contains the OCSP Responder Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the OCSP Responder Certificate.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	Issued monthly or more frequently with a validity period no longer than 45 days from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; contentCommitment, digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; optional; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA

10.1.7 SCVP Server Certificate

The following table contains the SCVP Server Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the SCVP Server Certificate.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 SCVP Server (subject) DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; contentCommitment, digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	HTTP URL for the SCVP Server

10.1.8 TSA Certificate

The following table contains the TSA Certificate profile assuming that the Root CA issues the TSA Certificate.

Field	**Value**
Version	V3 (2)

Field	Value
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than issuing Root-CA (up to 20 years)
Subject Distinguished Name	Unique subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	critical=no; <SKI of issuing CA's Signing Certificate>
Subject Key Identifier	c=no; <created at certificate issuance>
Key Usage	c=yes; digitalSignature, contentCommitment
Extended Key Usage	c=yes; id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
Certificate Policies	c=no; Policy OID from issuing CA
Authority Information Access	c=no; caIssuers: <from issuing CA> OCSP: <optional from issuing CA>

10.2 End-Entity Certificates

This section describes the values that populate each field of the Certificates issued by the Air Canada PKI CAs.

10.2.1 Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}

Field	**Value**
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; digitalSignature (always present)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; URI (mandatory if cardAuth is present, otherwise optional), otherName::principalName (1.3.6.1.4.1.311.20.2.3, optional, ASN1encoded UTF-8 string); RFC822 email address (optional); directoryName (optional); others optionalc=no; URI (optional), otherName::principalName(1.3.6.1.4.1.311.20.2.3, optional, ASN1-encoded UTF-8 string); RFC822 email address (optional); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no
Microsoft Directory Service {1.3.6.1.4.1.311.25.2}	c = no; optional; user AD SID

10.2.2 Subscriber Signature Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (always present)
Extended Key Usage[9]	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; RFC822 email address (required); URI (optional); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

[9] Included to support EKU for Smart Card Logon

10.2.3 Subscriber Encryption Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[10]	c=no; As per section 7.1.6
Subject Alternative Name	c=no; RFC822 email address (required); URI (optional), others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

[10] Only software OID asserted to support key recovery to software tokens

10.2.4 CIV Card Authentication Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049
Subject Distinguished Name	serialNumber=<GUID> with applicable DN prefix.
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; URI urn:uuid:<32 character hex representing 128 bit GUID>
CRL Distribution Points	c = no;
Authority Information Access	c = no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.5 CIV Content Signer Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	10 years from date of issue expressed in UTCTime for dates until end of 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	optional; c=no
CRL Distribution Points	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.6 Code Signing Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	expressed in UTCTime until 2049. As per section 5.6 of this CP
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (optional)
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; DN of the person controlling the Code Signing Private Key
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.7 Device or Server Identity Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (required), keyEncipherment (optional)
Extended key usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; optional if FQDN is in the Subject Distinguished Name's CN otherwise required: Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.8 Device or Server Signature Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (optional)
Extended key usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; optional, RFC822 email address | Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.9 Device or Server Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[11]	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

[11] Only software OID asserted to support key recovery to software tokens

10.2.10 Aircraft or Aircraft Equipment Identity Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (required), keyEncipherment (optional)
Extended key usage	c=no; as per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed byLDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.11 Aircraft or Aircraft Equipment Signature Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (optional)
Extended key usage	c=no; as per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.12 CSCT Signing Services Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 5 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (optional)
Extended key usage	c=no; as per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.13 Aircraft or Aircraft Equipment Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended key usage	c=no; as per section 10.7
Certificate Policies[12]	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed byLDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

[12] Only software OID asserted to support key recovery to software tokens

10.2.14 Role Signature Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN for role conforming to Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), contentCommitment (always present)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c = no; DN of the person controlling the role signing private key; RFC822 email address of role (Optional)
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA

Field	Value
	OCSP Responder

10.2.15 Role Encryption Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN for role conforming to Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[13]	c=no; As per section 7.1.6
Subject Alternative Name	c = no; DN of the person controlling the role private key; RFC822 email address of role (required); others optional
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

[13] Only software OID asserted to support key recovery to software tokens

10.3 CRL Format

10.3.1 Full and Complete CRL

If the CA provides OCSP Responder Services, the CA shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date (in Generalised Time)
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-sha256 {1.2.840.10045.4.3.2}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in Certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise
Hold Instruction	c=no; optional, id-holdinstruction-reject[14]

10.3.2 Distribution Point Based Partitioned CRL

Not Supported.

[14] may be present only if reason code = certificateHold

10.4 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 6960 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of Certificates as specified in RFC 6960
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.5 OCSP Response Format

See [RFC 6960] for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	**Value**
Response Status	As specified in RFC 6960
Response Type	id-pkix-ocsp-basic {1.3.6.1.5.5.7.48.1.1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder Certificate)
Produced At	Generalised Time
List of Responses	Each response will contain Certificate id; Certificate status[15], thisUpdate, nextUpdate[16],
Responder Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11} or ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
Certificates	Applicable Certificates issued to the OCSP Responder
Response Extension	**Value**

[15] If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

[16] The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

Field	Value
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**
None	None

10.6 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests.

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP.
Subject Public Key Information	Refer to section 6.1
Subject's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, digitalSignature, contentCommitment
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC822, and DNS name forms

10.7 Permitted Extended Key Usage Values

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA[17]	None	None	All

[17] CA Certificate includes: self-signed Root Certificate, Cross-Certificates, Intermediate and tier-1 Subordinate CA Certificates, and self-issued key rollover Certificates.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Subordinate CA (tier-2) (BEGSS and E-EGS)	id-kp-serverAuth {1.3.6.1.5.5.7.3.1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
OCSP Responder	id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}	None	All Others
SCVP Server	id-kp-scvpServer {1.3.6.1.5.5.7.3.15}	None	All Others
Subscriber, Role: Authentication	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1.3.6.1.5.2.3.4}[18]	Any EKU that is consistent with Key Usage	anyExtendedKeyUsage {2.5.29.37.0}; and Any EKU that is not consistent with Key Usage
Subscriber, Role: Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; MSFT Document Signing {1.3.6.1.4.1.311.10.3.12}; Adobe Certified Document Signing {1.2.840.113583.1.1.5}	Any EKU that is consistent with Key Usage	anyExtendedKeyUsage {2.5.29.37.0}; and Any EKU that is not consistent with Key Usage
Subscriber, Role: Encryption[19]	id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	anyExtendedKeyUsage {2.5.29.37.0}; and Any EKU that is not consistent with Key Usage
CIV Card Authentication	id-eku-civ-cardAuth {1.3.6.1.4.1.49507.1.10.1}	None	All Others
CIV Content Signing	id-eku-civ-content-signing {1.3.6.1.4.1.49507.1.10.2}	None	All Others

[18] smartCardLogon and id-pkinit-KPClientAuth required only if the private key is in hardware.

[19] This Certificate is defined as the one that has only the key encipherment or key agreement bit set and optionally data encipherment bit set.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Code Signing	id-kp-codesigning {1.3.6.1.5.5.7.3.3}	Life-time Signing {1.3.6.1.4.1.311.10.3.13}[20]	All Others
LSAP Signing (for CSCT Signing use)	id-eku-boeing-lsap-code-signing {1.3.6.1.4.1.73.15.3.1.42.42}	None	All Others
Device Authentication, Web Server	id-kp-serverAuth {1.3.6.1.5.5.7.3.1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Device Document Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4} Adobe Certified Document Signing {1.2.840.113583.1.1.5}	Any EKU that is consistent with Key Usage, e.g., MSFT Document Signing {1.3.6.1.4.1.311.10.3.12};	anyExtendedKeyUsage {2.5.29.37.0}; and Any EKU that is not consistent with Key Usage
Device Email Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}	Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage
Device Encryption	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	anyExtendedKeyUsage {2.5.29.37.0}; and Any EKU that is not consistent with Key Usage
Domain Controller	id-kp-serverAuth {1.3.6.1.5.5.7.3.1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-pkinit-KPKdc {1.3.6.1.5.2.3.5}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}	None	All Others
Time Stamp Authority	id-kp-timestamping {1.3.6.1.5.5.7.3.8}	None	All Others

[20] It is recommended that this EKU be included so that Microsoft platforms will not verify signed code using an expired Certificate.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
VPN	id-kp-serverAuth {1.3.6.1.5.5.7.3.1}	None	All Others
Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Workstation	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1.3.6.1.5.5.7.3.17}	None	All Others