Carillon Information Security Inc. Public Key Infrastructure

Certificate Policy

CIS-POL-0007

Validation and signature of the PMA CHAIR:

Patrick Patterson - SIG

Digitally signed by Patrick Patterson - SIG
Date: 2024.01.15 15:26:07 -05'00'

Author: Carillon Information Security Inc.

Date: January 15, 2024
Version: 2.3
Classification: **PUBLIC**
Status: **FINAL**

Version Information

Version number	Date	Author	Notes
0.1		Vince Chiarelli Patrick Patterson	Initial Draft
1.0	2012-08-30	Donata De Luca / Patrick Patterson / Patrick Turcotte / Pierre Pavlenyi	Final Initial Version
1.1	2012-09-10	Dave Coombs / Donata De Luca / Patrick Patterson / Pierre Pavlenyi / Vince Chiarelli	Entry in operation
1.2	2012-11-22	Donata De Luca	Fix section numbering; Correct spelling errors; Include name space control enforcement mechanism.
1.3	2013-08-08	Pierre Pavlenyi / Donata De Luca	Editorial cleanup; Reduce IceCAP Content Signer key lifetime from 4 years to 3; Reduce IceCAP Content Signer Certificate lifetime from 10 years to 9. Addition of Assurance Levels: basic-hardware, basic-hardware-256, medium-softwareCBP, and medium-hardwareCBP Changes to OID #s: medium-softwareCBP, medium-hardwareCBP, and basic-software-256 Define that TA is appointed by OA; Permit digital signature of declaration of identity; Alignment with CertiPath policy. Change nextUpdate for Root and Bridge CA CRLs to thisUpdate plus 45 days; Change nextUpdate for other CA CRLs to

Version number	Date	Author	Notes
			thisUpdate plus 48 hours. Change LDAP publication from mandatory to optional. Clarification of terminology, including: replace "PKI Sponsor" with "Device Sponsor". Correct spelling; Update CP and Privacy Policy URLS. Modification to Key Pair generation and escrow requirements, name forms, and inclusion of Aircraft and Aircraft Equipment Certificate Profiles. Change Issuer Signature Algorithm and Issuer Signature fields of PCA -> CBCA G2 Certificate profiles to SHA256 only. Replaces instances of "Federal PIV" with "United States Federal Government PIV".
1.4	2013-12-06	Donata De Luca	Add new assurance levels CIS-INFRASTRUCTURE and CIS-INFRASTRUCTURE-256; Addition of CBP-256 assurance levels and related exemptions; Update definitions and acronym list; Correct spelling of sha1WithRSAEncryption and sha256WithRSAEncryption; and Various changes to align with CertiPath CP.
1.5	2014-02-07	Donata De Luca	Include IceCAP in acronym list; Correct IceCAP-cardAuth position in hierarchy diagram; Remove exemption of background checks for CBP; Exempt citizenship of Trusted Roles for CBP-only CAs; Include all Medium Assurance Levels in the requirement against existence private key in plaintext form outside of its cryptographic module; Clarify key generation requirements for aircraft; Add communication of compliance results

Version number	Date	Author	Notes
			requirements; Correction to URL of CP.
1.6	2014-03-14	Donata De Luca	Allow modification of IceCAP-contentSigning Certificates.
1.7	2014-04-18	Donata De Luca et al.	Align with latest version of Spec 42 CP for Role-Based Code Signing Certificates used for signature of Aircraft software/parts.
1.8	2014-08-06	Nabila Nouaouria	Add TSA information in section 1.6. Add Information about Role Identity, SCVP Responders and TSA in section 5.6. Add Information about SCVP Responders and TSA in section 6.1.1. Add SCVP Certificate profile in section 10.1.6. Add TSA Certificate profile in section 10.1.7. Add of Role Identity Certificate profile in section 10.2.11. Update the EKU table in section 10. Add an EKU value for SCVP Responder to the EKU table in section 10.7. Add an EKU value for Boarding Pass Signing to the EKU table in section 10.7.
1.9	2015-03-19	Nabila Nouaouria / Patrick Turcotte	Alignment on CertiPath CP, customer requirements and minor corrections: Add content in sections 1.3.1.8, 1.6.2, 4.9.1, 5.6, 6.1.1, 6.1.5, 10.2.7, 10.2.13 and 10.7. Remove contents from sections 3.2.1, 4.5.2, 4.6, 4.8, 4.8.1, 5.3.1, 10.1.1, 10.1.2 and 10.1.4. Modify content in sections 5.2.2, 5.6, 6.1.1, 6.2.1, 10.1.4, 10.2.4, 10.2.10 and 10.7.
1.10	2015-09-28	Patrick Turcotte / Nabila Nouaouria / Lyne Brosseau	CR-01 - Alignment on Spec 42 and CertiPath: Modify contents in sections 3, 4, 5, 6, 7 and 8. CR-02 - Alignment on Spec 42 and CertiPath: Modify content in section 10.7 CR-03 - Alignment on Spec 42 and CertiPath: Modify contents in sections 1.2 and 7.1.6 CR-04 - Alignment on Spec 42 and CertiPath: Modify content in section 10. CR-05 - Add a Document References section

Version number	Date	Author	Notes
			and Minor editorial changes.
1.11	2016-02-17	Carillon Information Security	CR-01 – Minor Adjustments: Modify contents in sections 1.2 and 4.1. CR-02 - Adjustments for CertiPath compliance: Add content in sections: 1.3.1.8, 7.1.6, 10 and 10.6. Modify contents in sections: 3.2.3.1, 3.4, 4.5.2, 5.4.8, 6.1.5, 10.2.1 to 10.2.13 and 10.7 Delete content in sections: 3.2.1 and 6.1.7. CR-03 – Reference update: Modify contents in sections 1.6.1 and 3.2.3.1.
1.12	2016-02-23	Carillon Information Security	CR-01 – Minor Adjustments: Modify contents in sections: reference table, 1.2, 1.3.3, 6.2.4.1, 6.8 and 7.1.6. CR-02 – Addition of Certificate suspension requirements: Add section 3.2.3.5. Modify contents in sections: 4.913 to 4.9.16 and section 10.3.1.
1.13	2016-08-31	Carillon Information Security	CR-01 – Minor adjustments: Modify contents in sections: 6.1.4 and 10.2.14. CR-02 – Addition of CIV Certificate profiles: Add contents in sections: 1.6.2, 5.6, 6.1.1, 10.2 and 10.7. Modify contents in sections: 4.8, 4.8.2, 5.2.2, 5.6, 5.7.3, 6.2.2, 6.2.4.4 and 6.2.8. CR-03 – Changes to align on CFS Certificate Policy v.1.7 following TSCP mapping exercise: Add content in sections: 2.1; 4; 4.3; 4.3.1; 4.9.3; 4.9.6; 4.9.8; 4.9.11; 5.5.1; 5.5.7; 5.6; 5.7.3; 6.2.10; 6.6.1; 6.8; 8; 9.4; 9.6.2; 11.

Version number	Date	Author	Notes
			Modify contents in sections: 2.4; 3.11; 4.1.2.2; 4.9.1; 4.10; 4.12.1; 5.1.1; 5.2.1.5; 5.2.2; 5.4.5; 6.1.6; 6.2.3; 6.2.5; 8.5; 9.2.1; 9.6.1.2. CR-04 – Changes to complete the TSCP mapping exercise: Add content in section: 9.9.2 Modify contents in sections: 7.1.6; 9.8; 9.16.5
1.14	2016-11-16	Carillon Information Security	CR-01– Minor adjustments Modify content in section: 10.2.6. CR-02 – Changes to conform to Certipath CP 3.28 Add content in sections: 1; 1.2 and 7.1.6. Modify content in sections: 1.3.6; 3.3.1; 4.9.13; 6.1.1; 6.4.1 and 11.
1.15	2017-01-11	Carillon Information Security Inc.	CR-01– Minor adjustments CR-02 - Modify content in section: 9.6.3 Modify a reference. CR-03 - Modify content in section: 4.12.1 Modify the requirements for key escrow CR-04 - Modify content in section 5.3.2: increase the refresh interval of background checks to every 3 years. CR-05 – Modify content in section Document References: Removal of Document References table
1.16	2017-02-20	Carillon Information Security Inc.	CR-01 – Minor adjustments CR-02 – Extension of KRPS approval Modify content in section: 4.12.1 CR-03– CertiPath compliance adjustments Modify content in sections: 1.3.6; 1.4; 1.6.1; 4.9.3; 4.9.5; 4.9.16; 6.1.7; 7.1.6; 10.1.4; 10.2.3; 10.2.5; 10.2.7; 10.2.8; 10.2.10; 10.2.13; 10.7.

Version number	Date	Author	Notes
1.17	2017-06-01	Carillon Information Security Inc.	CR-01 – Minor adjustments CR-02 - Modify requirement for in-person proofing Modify content in section 3.2.3.1
1.18	2017-12-07	Carillon Information Security Inc.	CR-01 – Minor adjustments Modify content in the following sections: 3.2.3.1; 6.1.7; 10.1.1. CR-02 – Adjustments required for the issuance of LSAP Signer Certificates Modify or add content in the following sections: 1.6.2; 3.2.3.4; 4.7.2; 4.7.3; 4.9.2; 5.6; 6.1.1; 6.3.3; 7.1.6; 10.2.5; 10.7. CR-03 – Clarification of the CA actions during Certificate issuance Modify content in the following section: 4.3.1 CR-04 – Removal of sha1 Remove content in the following sections: 7.1.3; 10.1.2; 10.1.3; 10.1.4; 10.2.1; 10.2.2; 10.2.3; 10.2.4; 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. CR-05 – CertiPath CP v.3.32 compliance adjustments Add or modify content in the following sections: 1.3; 1.3.1; 1.6.2; 2.4; 4.9.16; 5.1.1; 5.1.2.1; 5.2.3; 5.4.1; 5.4.2; 5.4.3; 5.5.1; 5.7; 6.1; 6.5.1; 6.6.2; 6.7; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5; 10.1.6; 10.1.7; 10.2.1; 10.2.2; 10.2.3; 10.2.4; 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; 10.2.15; 10.2.16; 10.2.17; 10.2.18; 10.3.1; 10.5; 10.6.

Version number	Date	Author	Notes
			CR-06 - TSA Certificate profile modifications for SPEC42 compliance Modify the following sections: 10.1.6; 10.1.7.
1.19	2019-01-07	Carillon Information Security Inc.	CR-01 – Remove incorrect information in the following section: 3.1.2 Throughout the document – Minor typographical adjustments CR-02 – CertiPath CP v.3.34 compliance adjustments Modify or add content in the following sections: 1.3.1.1; 4.4.3; 4.9.1; 4.9.13; 5.7.1; 5.7.2; 5.7.3; 5.8; 7.1.4; 9.11; 10.2.17; 10.7; 11. CR-03 – Alignment to Federal Bridge PKI requirements Add content in the following section: 1.3.1.4. CR-04 – Alignment to SPEC42 requirements Add a subsection in the following section: 2.2. CR-05 – Removing the requirement for backing up Content Signing Keys Modify content in the following section: 6.2.4.4. CR-06 – Modification concerning the publication of public encryption Certificates Modify content in the following section: 2.2.1. CR-07 – Modification to section regarding interoperability to remove unnecessary information Modify content in the following section: 2.2.2. CR-08 – Modification concerning the authentication of organisation identity.

Version number	Date	Author	Notes
			Remove content in the following section: 3.2.2. CR-09 – Add a new Certificate profile and its associated EKU. Add content in the following sections: 10.2; 10.7.
1.19a	2019-02-07	Carillon Information Security Inc.	Correction of involuntary line removal in section 3.2.6
1.20	2019-07-25	Carillon Information Security Inc.	CR-01: Minor adjustments Modify references to the CIS Root CA to allow for the possibility of the existence of several CIS Root CAs. Adjustments to conform to the Documented Information Policy and Documented Information Procedures documents. Removal of an obsolete reference. Throughout the document – Minor typographical and formatting adjustments. CR-02: Modify to accommodate new encryption role and device Certificates Modify or add content in the following sections: 1.3.6; 3.2.3.2.2; 3.2.3.4; 4.7.3; 5.2.1.9; 6.2.3; 7.1.6; 10.7 CR-03: Specifically allow the PMA to authorize the use of non-CIS-issued Certificates Modify content in the following section: 5.2.1.9 CR-04: Cross-Certificate profile modification Modify content in the following section: 10.1.1 CR-05: Device License Signing Certificate profile and EKU name modification Modify content in the following sections: 10.2.9; 10.7 CR-06: CIV Content Signer profile

Version number	Date	Author	Notes
			modification Modify content in the following section: 10.2.19
1.21	2019-12-20	Carillon Information Security Inc.	CR-01: Minor adjustments Remove content in the following sections: 6.7; 9.6.1.2 Throughout the document – Minor typographical and formatting adjustments. CR-02: Replace the figure called Carillon PKI Domain to reflect the new CIS PKI infrastructure Modify content in the following section: 1.1.4 CR-03: Add the 2 new "aero" assurance levels Modify or add content in the following sections: 1; 1.2; 1.3.6; 3.2.3; 3.3.1; 4.9.5; 6.1.1; 6.2.4.2; 7.1.6 CR-04: Changes required for CertiPath CP v. 3.38 compliance Modify or add content in the following sections: 1.6.1; 1.6.2; 3.2.3.1; 6.1.5; 6.2.4; 6.2.8; 9.4; 10.1 CR-05: Changes for operational consistency and business development Modify or add content in the following sections: 1.3.1.1; 1.6.1; 1.6.2; 4.4.3; 4.9.1; 4.10.2; 5.5.2; 5.8; 6.2.4.; 6.5.1; 9.4; 9.11; 10; 10.1, 11
1.22	January 21, 2020	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02: Inclusion of a new Root CA Modify content in the following section: 1.1.4

Version number	Date	Author	Notes
1.23	January 30, 2020	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02: Changes required for CertiPath CP v. 3.38 compliance Modify or add content in the following sections: 1.3.6; 6.1.5; 6.2.4.4
1.24	August 11, 2020	Carillon Information Security Inc.	CR-01: Minor adjustments Remove content in the following section: 10.2.2 Throughout the document – Minor typographical and formatting adjustments. CR-02: Increase repository availability from 99% to 99.9% Modify content in the following section: 2.1 CR-03: Modify the name of the CertiPath CA in the section title and its profile Modify content in the following section: 10.1.1 CR-04: Change contentCommitment to nonRepudiation Modify content in the following sections: 6.1.7; 10.1.7; 10.1.8; 10.6 CR-05: Add a definition for Sunset Date Add content in the following section: 1.6.1 CR-06: Add requirements related to the Signature Trust Platform (STP) Modify or add content in the following sections: 1.3.1; 1.3.1.11; 1.6.1; 1.6.2; 5.1.1; 5.1.2.1; 5.2.1; 5.2.4; 5.3.1; 5.3.2; 5.3.3; 5.3.4; 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; 5.5.3; 5.7.1; 6.1.1; 6.2.1; 6.2.4; 6.2.6; 6.2.8; 6.4.1; 6.4.2; 6.4.3; 6.5.1; 6.6.1; 6.6.2; 6.7; 6.8;

Version number	Date	Author	Notes
			9.6.5 CR-07: Changes required for SAFE cross-certification Modify or add content in the following sections: 1.3.5; 2.4; 3.2.3.1; 3.3.1; 4.7.3; 5.2.1; 5.5.6; 5.8; 6.1.1; 6.2.6; 7.1.3; 9.6.2; 10.5 CR-08: Modification of the routine CRL issuance frequency from every 24 hours to every 18 hours Modify content in the following section: 4.9.7
1.25	August 18, 2020	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02: Change required for SAFE cross-certification Modify content in the following section: 6.1.6
1.26	December 8, 2020	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02: Change of authorized Level of Assurance for LSAP Role Certificates Modify content in the following section: 7.1.6 CR-03: Changes required for CertiPath CP v. 3.41 compliance Modify, add, or remove content in the following sections: 2.2.1; 3.2.3.1; 4.9.7; 4.9.9; 4.9.10; 4.9.15; 5.6; 6.1.5; 10; 10.3.1; 10.5
1.27	January 14, 2021	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments.

Version number	Date	Author	Notes
			CR-02: Add requirements related to the Signature Trust Platform (STP) Add content in the following section: 7.1.6
1.28	February 17, 2021	Carillon Information Security Inc.	CR-01: Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02 - Add requirements related to the addition of 2 new "basic-device" Policy OIDs Add or modify content in the following sections: 1; 1.2; 1.3.6; 3.3.1; 4.9.5; 6.1.1; 6.4; 7.1.6 CR-03: Modify the Sub CA Certificate life times Modify content in the following section: 5.6
2.0	December 16, 2021	Carillon Information Security Inc.	CR-01 - Minor adjustments Throughout the document – Minor typographical and formatting adjustments. CR-02 - Changes required for CertiPath CP v. 3.44 compliance Modify, add, or remove content in the following sections: 4; 5.3.1; 5.3.2; 6.1; 6.2.1; 6.2.7; 7.1.3; 10; 10.1; 10.2; 10.3.1; 10.5; 10.6 CR-03 - Removal of deprecated Policy OIDs Modify and remove content in the following sections: 1; 1.1.4; 1.2; 1.3.5.3; 1.3.6; 3.2.3.1; 3.2.3.2; 3.3.1; 4.1.1.2; 4.1.2.1; 4.9.5; 5.2; 5.3; 5.3.1; 5.4; 5.5; 6.1.1; 6.2.4.2; 7.1.6; 8.1; 8.2; 8.3 CR-04 - Modify the allowed policy OIDs for Role Encryption Certificates Modify content in the following section: 7.1.6

Version number	Date	Author	Notes
			CR-05 - Modify Certificate lifetimes Modify content in the following section: 5.6 CR-06 - Removal of SCVP servers from list Modify content in the following section: 1.2 CR-07 - Add information about the octet string calculation Add content in the following section: 10
2.1	December 16, 2022	Carillon Information Security Inc.	CR-01 - Minor adjustments Correct minor omissions and modify erroneous content. Modify content in the following sections: 3.2.3.5; 6.11; 6.1.3; 6.4.1; 6.4.3; 7.1 Throughout the document – Minor typographical and formatting adjustments CR-02 - Clarifications regarding the Key Usage Purposes Addition of a reference to Certificates issued to Human Subscribers Addition of an exception for OCSP Responder Certificates Add content in the following section: 6.1.7 CR-03 – 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 CR-04 – Addition of the optional Microsoft Directory Service extension in subscriber ID Certificates Add content in the following section1: 10.2.1 CR-05 – Addition of optional EKUs in encryption Certificates

Version number	Date	Author	Notes
			Add content in the following section: 10.7 CR-06 – Addition of new subsection 8.7 Add content in the following section: 8
2.2	December 21, 2023	Carillon Information Security Inc.	CR-01 - Minor adjustments Modify content in the following sections: 7.3; 9.3; 9.4; 10.1.6; 10.1.7; 10.6 CR-02 – Removal of requirements related to SIBCA Cross-Certification Remove content in the following sections: 7.1.6; 10.1 CR-03 – Modification of the SCVP Certificate profile Modify content in the following section: 10.1.5 CR-04 – Changes required for CertiPath CP v. 3.47 compliance Modify, add or remove content in the following sections: 1; 1.3.1.11; 1.4.1; 1.4.2; 1.5.3; 1.6.2; 2.2; 2.2.1; 2.2.2; 2.3; 2.4; 3.1.1; 3.1.2; 3.1.3; 3.2.3; 3.2.3.1; 3.2.3.2; 3.2.3.3; 3.2.4; 3.3.1; 3.3.2; 4.1.2; 4.2.1; 4.2.2; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.6; 4.6.1; 4.6.2; 4.6.3; 4.7; 4.7.2; 4.8; 4.8.3; 4.9.2; 4.9.3; 4.9.5; 4.9.8; 4.10; 4.10.1; 4.10.2; 4.10.3; 5.1.4; 5.1.5; 5.2.1.5; 5.2.1.6; 5.2.1.7; 5.3.3; 5.3.5; 5.3.8; 5.4; 5.4.1; 5.4.2; 5.4.3; 5.4.4; 5.4.6; 5.4.7; 5.4.8; 5.5.1; 5.5.2; 5.5.3; 5.5.5; 5.6; 5.7.1; 5.7; 5.7.2; 5.7.3; 5.7.4; 6.1.1; 6.1.4; 6.1.5; 6.1.6; 6.1.7; 6.2.1; 6.2.4.2; 6.2.6; 6.2.8; 6.2.10; 6.4.3; 6.5.2; 6.6.2; 6.6.3; 7.1.2; 7.1.4; 7.1.6; 7.1.7; 7.1.9; 7.1.10; 7.3; 7.3.2; 9.6.3; 9.12.2; 10.1.1; 10.1.3; 10.1.4; 10.6; 11

Version number	Date	Author	Notes
2.3	January 15, 2024	Carillon Information Security Inc.	CR-01 - Minor adjustments Standard upkeep for new version CR-02 – Update of aircraft-related device certificate profiles Modify content in the following sections: 10.2.10; 10.2.11; 10.2.12 CR-03 – Removal of FIPS requirements for basic-hardware assurance levels and table cleanup Modify content in the following section: 6.1.1 CR-04 – Expansion of nonRepudiation to SCVP and TSA Add content in the following section: 6.1.7 CR-05 – Update of device encryption certificate profile Add content in the following section: 10.2.8 CR-06 – Updates for CertiPath mapping Modify content in the following sections: 1.3.1.11, 2.2.1, 4.3.1, 5.2.1.7, 5.3.5, 6.1.7, 6.5.1, 9.6.3, 11

Document References

Document references found throughout this Certificate Policy are listed in the CIS 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-device-software-256
- basic-hardware-256,
- basic-device-hardware-256
- medium-softwareCBP-256,
- medium-aero-software-256
- medium-software-256,
- medium-device-software-256,
- medium-hardwareCBP-256,
- medium-aero-hardware-256
- medium-hardware-256,
- medium-device-hardware-256,
- IceCAP-cardAuth,
- IceCAP-hardware,
- IceCAP-contentSigning.

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 Carillon Information Security Inc. PKI, hereafter referred to as the Carillon 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 Carillon Root CAs and the certified subordinated Carillon Sub CAs. The Carillon Principal CAs (PCAs) may cross certify with other PKI domains in order to allow interoperation with other PKIs required for the business of Carillon Information Security Inc., its Business Units, affiliated companies, and customers.

Any use of or reference to this CP outside the purview of the Carillon PKI is completely at the using party's risk. Only the Carillon Root CAs and Sub CAs of those roots shall assert the OIDs listed in section 1.2 of this document in any Certificates issued by the Carillon

PKI, except in the policyMappings extension of Certificates issued by the CAs cross-certified with a Carillon PCA for the establishment of equivalency between Carillon 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 Carillon 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 a Carillon PCA shall, in the policyMappings extension and in whatever other fashion is determined by the Carillon Policy Management Authority (Carillon 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 a Carillon PKI CPS

This CP states what assurance can be placed in a Certificate issued under this policy. The Carillon Certification Practice Statements (Carillon CPSs) state how the Carillon 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 Carillon Policy Management Authority (Carillon PMA) to the levels of assurance of the Certificates issued by other PKI domains which cross certify with a Carillon PCA. The policy mappings information is placed into the Certificates issued by a Carillon PCA, or otherwise published or used by the Carillon 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.

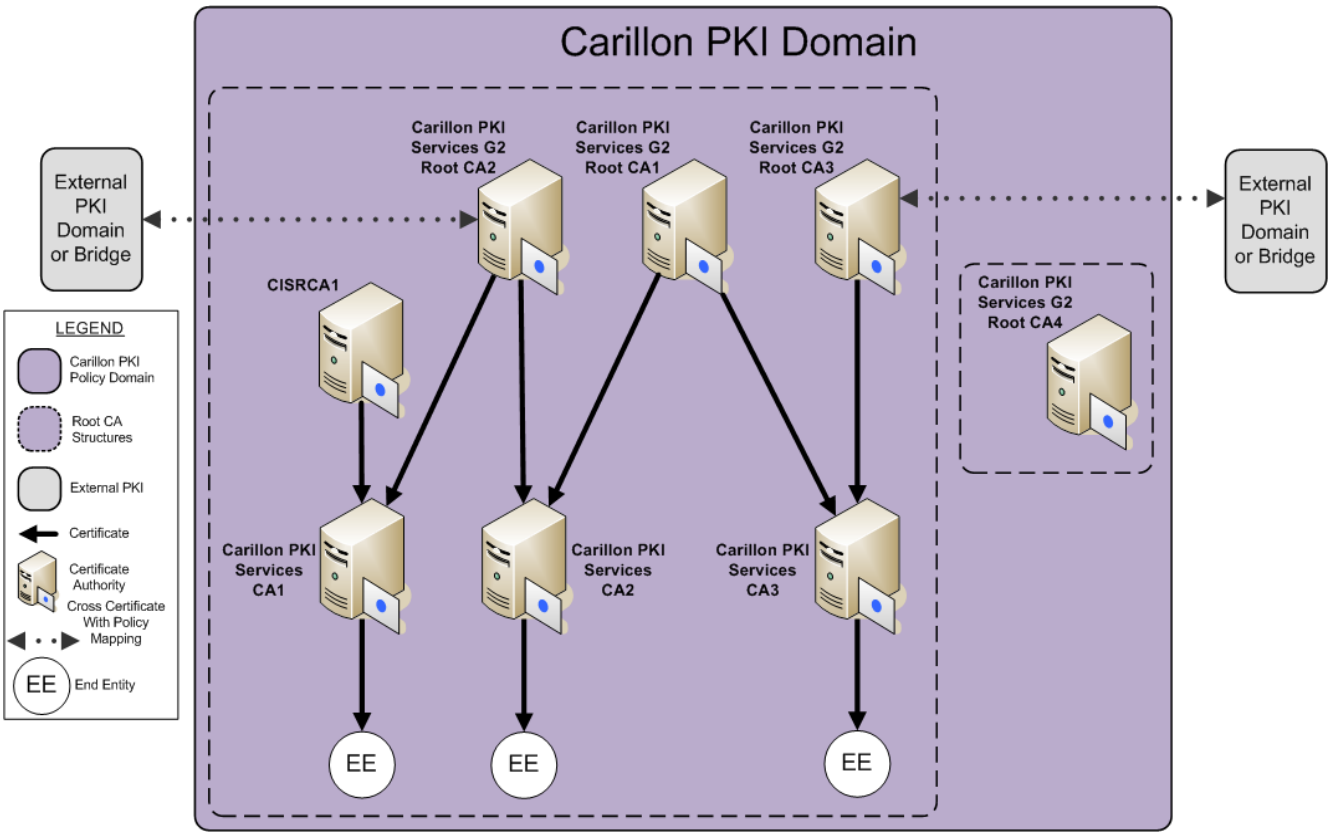

Figure 1 – Scope and Domain of Carillon CAs

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

- the Carillon Root Certification Authorities (Carillon Root CAs);
- all Carillon Certification Authorities subordinated to a Carillon Root CA (Carillon Sub CAs);
- other PKI domains' CAs.

The Carillon Root CAs shall issue CA Certificates only to Carillon Sub CAs approved by the Carillon PMA.

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

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

Carillon Sub CAs may issue Certificates to individuals, roles, or devices (including ground systems, aircraft, and aircraft avionics) at any Assurance Level consistent with the

Assurance Levels and type delegated to that Sub CA by its issuing CA.

The Carillon Root CAs and Carillon Sub CAs exist to facilitate trusted communications within the Carillon Domain and with Carillon 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 Carillon Root CAs and Carillon Sub CAs.

The term Carillon Sub CAs shall refer to any Sub CA within the Carillon PKI operated by Carillon, including but not limited to those operated on behalf of customers who have entered into a contractual relationship with Carillon.

Requirements that apply to a specific CA type will be denoted by specifying the CA type, e.g., Carillon Root CAs, Carillon Sub 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 Carillon Information Security Inc. 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 Carillon Sub CAs that complies with the policy stipulations under this CP.

The IceCAP assurance levels enable the issuance of smart cards that are technically interoperable with United States Federal Government Personal Identity Verification (PIV) Card readers and applications as well as PIV Interoperable (PIV-I) card readers and applications. See section 11 for more details.

An additional policy OID is used to distinguish the Content Signer within the IceCAP framework, and another additional policy OID is used to identify a Card within the IceCAP framework. The IceCAP-contentSigning policy is reserved for Certificates used by the Card Management System (CMS) to sign the IceCAP card security objects.

The requirements associated with the "id-basic-device…" and "id-medium-device. . ." policies are identical to those defined for equivalent non-device assurance policies with the exception of identity proofing, backup and activation data. The use of these policies is restricted to devices and systems (e.g. software applications and hardware devices).

With the exception of Certificates issued to aerospace devices, Certificates issued to end-entity devices at a basic assurance policy shall assert one of the following policies: id-basic-device-software-256 or id-basic-device-hardware-256.

With the exception of content-signers and OCSP responders, Certificates issued to end-entity devices at a medium assurance policy shall assert one of the following policies: id-medium-device-software-256 or id-medium-device-hardware-256.

The medium-aero-software-256 and medium-aero-hardware-256 Assurance Levels are for use by the aerospace community and allow for video-based identity proofing, per the recommendations of ATA Spec 42.

The OIDs are registered under the Carillon arc as follows:

Certificate Name	OID
id-carillon	::= {1.3.6.1.4.1.25054}
id-security	::= {id-carillon 3}
id-commercial-pki	::= {id-security 1}
id-CISINFRASTRUCTURE - DEPRECATED	::= {id-commercial-pki 1}
id-CISINFRASTRUCTURE-256 - DEPRECATED	::= {id-commercial-pki 2}
id-basicSoftware - DEPRECATED	::= {id-commercial-pki 3}
id-basicHardware - DEPRECATED	::= {id-commercial-pki 4}
id-mediumSoftwareCBP - DEPRECATED	::= {id-commercial-pki 5}
id-mediumHardwareCBP - DEPRECATED	::= {id-commercial-pki 6}
id-mediumSoftware - DEPRECATED	::= {id-commercial-pki 7}
id-mediumHardware - DEPRECATED	::= {id-commercial-pki 8}
id-basicSoftware-256	::= {id-commercial-pki 9}
id-basicHardware-256	::= {id-commercial-pki 10}
id-mediumSoftware-256	::= {id-commercial-pki 11}
id-mediumHardware-256	::= {id-commercial-pki 12}
id-mediumDeviceSoftware-256	::= {id-commercial-pki 13}
id-mediumDeviceHardware-256	::= {id-commercial-pki 14}
id-mediumAeroSoftware-256	::= {id-commercial-pki 15}
id-mediumAeroHardware-256	::= {id-commercial-pki 16}
id-basicDeviceSoftware-256	::= {id-commercial-pki 17}
id-basicDeviceHardware-256	::= {id-commercial-pki 18}
id-iceCAPHardware	::= {id-commercial-pki 20}
id-iceCAPCardAuth	::= {id-commercial-pki 21}
id-iceCAPContentSigning	::= {id-commercial-pki 22}
id-mediumSoftwareCBP-256	::= {id-commercial-pki 30}
id-mediumHardwareCBP-256	::= {id-commercial-pki 31}

The Carillon 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 stated, a requirement stated in this CP applies to all Assurance Levels. In addition, unless otherwise stated, a requirement for the medium-hardware Assurance Level shall apply to all three IceCAP Assurance Levels.

IceCAP assurance levels shall use SHA 256 for generation of PKI objects.

Assurance Level enumerations are listed in section 7.1.6.

1.3 PKI PARTICIPANTS

This section contains a description of the roles relevant to the administration and operation of the Carillon 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 Carillon PKI Authorities

1.3.1.1 Carillon Policy Management Authority (Carillon PMA)

The Carillon PMA is responsible for:

- Commissioning, drafting and approving the Carillon PKI CP (this document);
- Commissioning compliance analysis, acting on recommendations resulting from analysis, and approving the Carillon PKI CPSs;
- Accepting and approving applications from entities desiring to cross-certify with a Carillon PCA;
- Ensuring continued conformance of the Carillon PKI CPSs with applicable requirements as a condition for continued securing of the Assurance Levels as stipulated in this CP;
- Managing the interoperation with other PKI domains' CAs;
- Providing notification of changes that have the potential to affect their operational environments to cross-certified entities at least two (2) weeks and one day prior to implementation and provide all new artefacts (CA Certificates, CRL DP, AIA URLs, etc.) produced as a result of the change to cross-certified entities within 24 hours following implementation; and
- Ensuring continued conformance of the Carillon PKI and other domains' PKI with applicable requirements as a condition for allowing continued interoperability with cross-certified CAs.

Carillon 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 Carillon PMA roles and responsibilities is provided in the Carillon

PKI Policy Management Authority Charter [Carillon PMA CHARTER].

1.3.1.2 Carillon PKI Operational Authority (OA)

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

1.3.1.3 Carillon PKI Operational Authority Administrator

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

The Administrator is selected by and reports to the Carillon PMA.

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

1.3.1.4 Carillon 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, a Carillon 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.

A Carillon Principal CA shall not have more than one intentional trust path to a directly or indirectly cross-certified CA, regardless of path validation results[1].

1.3.1.5 Carillon Root CAs

A Carillon Root CA is a trust anchor for Relying Parties trying to establish the validity of a

[1] Multiple trust paths created as a result of certificate renewal or CA rekey do not violate the single trust path requirement above.

Certificate issued by a Carillon Sub CA, whose chain of trust can be traced back to that specific Root CA.

A Carillon Root CA issues and revokes Certificates to Carillon Sub CAs upon authorisation by the Carillon PMA. As operated by the Operational Authority, a Carillon Root CA is responsible for all aspects of the issuance and management of those Sub 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 Sub CA Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

A Carillon Root CA may function as a PCA.

1.3.1.6 Carillon Subordinate CAs

The Carillon Sub CAs are all of the Carillon Signing CAs subordinate to a Carillon Root CA as defined below.

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, a Carillon 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. Examples of a CSA are:

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of Certificates.

- Server-based Certificate Validation Protocol (SCVP) Servers that validate certification paths and/or provide revocation status checking services.

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide Certificate validation services shall adhere to the same security requirements as repositories.

CAs that issue End-Entity Certificates at any of the IceCAP Assurance Levels must provide an OCSP Responder. Furthermore, the OCSP Responder(s) shall be issued CA-delegated Certificates in order to ensure interoperability with cross-certified partners.

A Carillon Root CA must not provide Certificate status via OCSP.

1.3.1.8 Time-Stamp Authority (TSA)

A TSA is an authority that issues and validates trusted timestamps. A TSA may be operated in conjunction with a CA or independent of a CA.

A TSA operated in conjunction with a Carillon CA shall be RFC 3161-compliant.

1.3.1.9 Card Management System (CMS)

The Card Management System is responsible for managing smart-card token content. In the context of this CP, the CMS requirements are mandatory for the IceCAP Assurance Levels and recommended for other Assurance Levels. CAs issuing IceCAP Certificates are responsible for ensuring that all CMSes meet the requirements described in this document. In addition, the CMS shall not be issued any Certificates that express the IceCAP-hardware or IceCAP-cardAuth policy OID.

1.3.1.10 Signature Trust Platform (STP)

The Private Keys for multiple Subscribers may be stored on a Signature Trust Platform, or STP, based on either a hardware security module (HSM) interfaced to a server, or a software-protected set of Private Keys in a controlled server environment. This allows the Subscribers to access their credentials from multiple workstations and locations, and with reduced need for local specialized software and/or hardware. For the purposes of this CP, any centralized aggregation of Subscriber private signature keys must comply with the requirements for an STP as specified in this CP.

1.3.1.11 Administration Workstation

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

The Carillon PKI does not use Administration Workstations. Administration Workstations and their associated requirements are only described in this document for mapping and clarification purposes.

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 his or her Public Key Certificate. An RA interacts with the CA to enter and approve the Subscriber Certificate request information. The Carillon Operational Authority acts as the RA for the Carillon Root CAs, and for Carillon PCAs when dealing with cross certification. It performs its function in accordance with the concerned Carillon CPS approved by the Carillon 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.

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

Carillon Sub CA Subscribers shall include Carillon employees, subcontractors' 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 Organizations

Subscriber Certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational 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 Carillon CAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute

authorities. The Carillon CPSs 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 Subscribers 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.

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 as defined in 5.2.1.

1.3.5.3 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 as defined in 5.2.1, but should have been issued a credential that is equal to or higher Assurance Level than the credential that they are sponsoring.

1.3.5.4 Role Sponsor

A Role Sponsor is a Subscriber responsible for the management activities pertaining to the Roles Certificates for which he/she is the sponsor. The Role Sponsor shall hold an individual Certificate in his/her own name issued by the same CA (or by another PKI approved by the CIS PMA) 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:

- Authorizing individuals for a Role Certificate;
- Recovery of private decryption keys associated with Role Encryption Certificates, when applicable;
- 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 as defined in 5.2.1.

1.3.6 Applicability

The sensitivity of the information processed or protected using Certificates issued by Carillon 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 basic-device-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 basic-device-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-softwareCBP-256 medium-aero-software-256 medium-software-256 medium-device-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.
medium-hardwareCBP-256 medium-aero-hardware-256 medium-hardware-256 medium-device-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.

IceCAP-cardAuth	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation pin is not practical. Certificates issued at the IceCAP-cardAuth Assurance Level shall only be issued for Card Authentication, as defined by [SP 800-73].
IceCAP-hardware or IceCAP-contentSigning	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 are stored in hardware at this assurance level. Certificates issued at the IceCAP-hardware Assurance Level shall only be issued to human Subscribers. Certificates issued at the IceCAP-contentSigning Assurance Level shall only be issued to the CMS for signing the PIV-I card security objects.

In addition to the above:

Role-Based Code Signing Certificates issued under this CP, in which the role is clearly indicated to be the signature of Aircraft software/parts, are relevant to environments where software is to be loaded onto an aircraft system, the integrity of the software needs to be assured, and the source organization of the software needs to be identified. Subscriber Private Keys shall be stored in hardware.

Role Encryption Certificates issued under this CP are used in environments where the confidentiality of the data must be assured, usually to a degree that precludes key escrow; this means that irrevocable Private Key loss is an understood and accepted risk. Subscriber Private Keys shall be stored in hardware and their associated Certificates shall assert the medium-hardware-256 assurance level.

Device Encryption Recovery Certificates issued under this CP are used in environments where the confidentiality of the data must be assured, usually to a degree that precludes key escrow; this means that irrevocable Private Key loss is an understood and accepted risk. Subscriber Private Keys shall be stored in hardware and their associated Certificates shall assert the medium-device-hardware-256 assurance level.

CIV Card Authentication and CIV Content Signing are Certificate formats used in the issuance of CIV credentials, defined in section 10.2. They are also identified by specific Extended Key Usage codes, as described in section 10.7. They are not Assurance Levels, and only assert the basic-hardware-256 Assurance Level.

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 Carillon PMA or the Carillon 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 Carillon CAs will issue digital Certificates to Subscribers for various uses. Examples include:

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

This list of usage for digital Certificates issued by Carillon CAs is not complete and may be extended.

The Carillon CAs may also issue the following:

- digital Certificates and other signed card information for use in PIV-I cards issued to Subscribers;
- digital Certificates and other signed card information for use in CIV cards issued to Subscribers; and
- digital Certificates for use in PKI infrastructure devices and/or by PKI personnel.

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

1.4.1 Appropriate Certificate uses

Appropriate Certificate uses are listed in Section 1.3.6.

1.4.2 Prohibited Certificate uses

Certificates asserting the IceCAP-cardAuth policy OID are used only to authenticate the hardware token containing the associated Private Key and shall not be interpreted as authenticating the presenter or holder of the token.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation administering the document

The Carillon PMA is responsible for all aspects of this CP.

1.5.2 Contact person

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

Patrick Patterson
Chair of the Carillon PKI PMA

Carillon Information Security
356 Joseph Carrier
Vaudreuil-Dorion, Quebec, CANADA
J7V 5V5

1.5.3 Person determining CPS suitability for the policy

The Carillon PMA shall commission an analysis to determine whether the Carillon PKI CPSs conform to the Carillon 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 analyst shall be 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 Carillon 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 Carillon PKI CPSs shall specify how this CP shall be implemented to ensure compliance with the provisions of this CP. The approval procedures for the CPSs shall be outlined in the [Carillon 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

Carillon PKI Directory - Publicly-accessible Repository.

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.

Affiliated Organization - Organizations that authorize affiliation with Subscribers of IceCAP Certificates.

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.

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 access 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.

CertiPath - CertiPath is a corporation whose purpose is to design, implement, maintain and market a secure Public Key infrastructure communications bridge, initially focused on the aerospace and defence industry.

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 Carillon 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.

Commercial Identity Verification (CIV) – a type of credential that uses the same technology as PIV and PIV-I but does not share the same policy or cross-certification requirements.

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 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 Carillon.

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. Smartcards 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).

I-9 form – An Employment Eligibility Verification form issued by the United States Department of Homeland Security whose purpose is to document verification of identity and employment authorization by employers. As used in the context of this CP, it is the basis for identity verification for the PIV-I enrollment process.

IceCAP – In the context of this CP, it is the name of the Assurance Levels required in the

PIV-I implementation.

Internet Engineering Task Force (IETF) - The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches 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 whose primary function is to issue Certificates to other CAs. 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 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.

Local Registration Authority (LRA) - An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).

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

Carillon consults the Carillon PMA through the Carillon 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 Carillon 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.

Personally Identifiable Information - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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 emphasizing 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 Group 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 Carillon 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 Carillon 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 authorized to act.

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

SAFE Identity – SAFE Identity is a corporation whose purpose is to design, implement, maintain and market a secure Public Key infrastructure communications bridge, focused on the pharmaceutical industry.

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.

Signature Trust Platform (STP) – A service designed to allow the remote, legitimate and secure use of a Subscriber's private signature key.

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.

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

Subject - The subject field of a Public Key Certificate identifies the entity associated with the public key stored in the subject public key field. Names and identities of a subject may be carried in the subject field and/or the subjectAltName extension. Where subject field is non-empty, it MUST contain an X.500 distinguished name (DN). The DN MUST be unique for each subject entity certified by a single CA as defined by the issuer name field.

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.

Sunset Date – Date at which a particular algorithm or cryptographic tool no longer meets the requirements of a specific context, and by which said algorithm or cryptographic tool must be completely phased out of that context.

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
AW	Administration Workstations
C	Country
CA	Certification Authority
CBCA	CertiPath Bridge Certification Authority
CBP	Commercial Best Practices
CHUID	Cardholder Unique Identifier
CIV	Commercial Identity Verification
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
DN	Distinguished Name
DNS	Domain Name Service
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End-Entity
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

IceCAP	Identity and Credential Assurance Policy
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
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
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)
SCEP	Simple Certificate Enrolment Protocol

SCVP	Server-based Certificate Validation Protocol
SHA-1	Secure Hash Algorithm, Version 1
SIBCA	Safe Identity Bridge Certificate Authority
SSCD	Secure Signature-Creation Devices
SSL	Secure Sockets Layer
STP	Signature Trust Platform
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TSA	Time-Stamp Authority
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 Carillon PKI operates Repositories containing all information necessary to provide lookup and validation services for issued Certificates.

The mechanisms used by the Carillon PKI to post information to its respective repositories, as required by this CP, shall include:

- Directory Server System that is also accessible via the Internet through the Lightweight Directory Access Protocol (LDAP) or 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 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 99.9% availability or better).

In cases where a CA has multiple repositories, the following rule shall apply to repository references within Certificates:

- All HTTP URI shall appear before LDAP URI.

2.2 Publication of Certificate information

2.2.1 Publication of CA Information

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

Unless otherwise specified in the Certificate profile or applicable CPS, all encryption Public Key Certificates issued by the Carillon CAs to digital Certificate users shall be published to the respective applicable Carillon Repositories, as set forth in the applicable CPSs.

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

With the exception of self-signed Certificates, all CA Certificates issued to a CA shall be published in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all Certificates issued by the CA.

With the exception of self-signed Certificates and those CA Certificates with the Basic Constraints path length constraint set to zero, after February 21, 2023, all new CA Certificates issued by the CA shall be published in a second file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA)

extension in all Certificates issued to the CA.

In both cases, the file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

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

All publication made by Carillon 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.

The latest CRL covering all unexpired Certificates shall be posted as a file available via a publicly accessible HTTP URI until such time as all issued Certificates have expired. This URI shall be asserted in the CRL distribution point extension of all Certificates issued by that CA, with the exception of OCSP responder Certificates that include the id-pkix-ocsp-nocheck extension.

CAs that provide OCSP must do so in the form of a publicly accessible delegated OCSP service, as described in Section 2.6 of RFC 6960. OCSP services must be designed and implemented to provide 99.9% availability or better, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

PRACTICE NOTE:

Internet disruptions may impact the response time experienced by the relying party.

2.2.2 Certificate Policy Publication

The CP shall be publicly available through the internet here:

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

2.3 Time or frequency of publication

Carillon 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 by that CA. Certificate Policy updates (revisions) shall be made publicly available within 30 days of approval. 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.

IceCAP Certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., HTTP, LDAP, etc.).

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The Carillon 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.

3.1.1.1 Subject Names

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

IceCAP-contentSigning Certificates shall clearly indicate the organization administering the CMS.

IceCAP-cardAuth Certificates' subject DN shall not contain the common name (cn). Instead, the DN shall populate the serialNumber attribute with the Universally Unique Identifier (UUID) associated with the card.

For IceCAP Certificates, with the exception of the IceCAP-contentSigning Certificate, the subject DN shall either contain the value "Unaffiliated" in the last organizational unit (ou) attribute or shall contain the affiliated organization name in an appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc) attribute).

If the subject DN includes the value ou = "Unaffiliated", the value ou = <Issuing CA CN> shall also be present.

For Certificates issued to devices, the subject DN must contain a unique name for the device that does not take the form of a Human Subscriber name.

3.1.1.2 Subject Alternative Names

Subscriber Certificates that contain an EKU value of id-kp-emailProtection shall include a rfc822Name in the Subject Alternative Name extension.

IceCAP-Hardware and IceCAP-cardAuth Certificates shall include a Subject Alternative Name extension containing a UUID value encoded as a URI.

IceCAP-cardAuth Certificates shall not include any name other than the UUID value in the Subject Alternative Name extension.

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.

- 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.);

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

The Subject Name in a CA Certificate must match the Issuer Name in Certificates it issues.

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

When UPN is used, it shall be unique and accurately reflect organizational structure.

3.1.3 Anonymity or pseudonymity of Subscribers

CA Certificates shall not contain anonymous or pseudonymous identities.

Certificates issued by Carillon CAs to Human Subscribers 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 [Carillon PKI Naming Policy], and in the applicable Certificate profile.

The authority responsible for Carillon PKI namespace control is the Carillon PMA.

3.1.5 Uniqueness of names

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

The applicable CPSs 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

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

names).

The Carillon PMA shall be responsible for ensuring name uniqueness in Certificates issued by the Carillon 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 Carillon 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 Carillon PMA may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of organisation identity

Requests for Certificates in the name of an organisation or corporation shall include the following:

- Full organisation legal 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.

In all cases, the existence of an affiliated organisation shall be verified prior to issuing an end user Certificates on its behalf. The RA shall verify the authenticity of the requesting representative and the representative's authorisation to act in the name of the organisation. 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.

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 authorization to act in the name of the CA.

3.2.3 Authentication of individual identity

The Carillon CAs shall ensure that the applicant's identity information is verified and checked in accordance with this CP and the applicable CPSs. 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.

The CA must authenticate the identity of the individual requestor for each Certificate issued.

In addition to the processes described below, Subscriber Certificates may be issued on the basis of an electronically authenticated request using a valid signature or authentication Certificate and associated Private Key, with the following restrictions:

- The assurance level of the new Certificate shall be the same or lower than the assurance level of the Certificate used to authenticate the request.
- Identity information in the new Certificate must match the identity information in the Certificate used to authenticate the request.
- The expiration date of the new Certificate shall not exceed the next required initial identity authentication date associated with the Certificate used to authenticate the request.
- The next initial identity authentication date remains unchanged in the event of a new Certificate issuance based on electronic authentication.

This electronic authentication process does not remove the requirement for periodic in-person identity proofing, as described in section 3.3.1.

3.2.3.1 Authentication of Human Subscriber Identity

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 Carillon PMA. If the data is used to proof an identity for medium-software or medium-hardware Assurance Level, 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:

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 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 applicant's Employer;
- a physical address or other suitable method of contact (which may be an email address);
- a declaration signed by the applicant indicating his 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 (which may be an email address);
- a declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4;
- 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;
- unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant or, in the case of electronic authentication, the serial number, subject key identifier, public key or other unique identifier from the Certificate used to authenticate the request;
- the identity of the person performing the identity verification; and either
  - 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; or
  - An auditable record linking the authentication of the person performing the identification to the verification of each Applicant; and
- the date and time of the verification.

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, one valid U.S. State REAL ID Act-compliant picture ID[3], or two valid non-National Government IDs, one of which shall be a recent photo ID. 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.

At the IceCAP-hardware and IceCAP-cardAuth Assurance Levels, the following additional requirements shall apply:

- In-person antecedent method shall not be used;
- Identity proofing shall be performed by an RA or a Trusted Agent only;
- The applicant shall present two identity source documents in original form. The identity source documents shall come from the list of acceptable documents included in FIPS 201-3 Section 2.7; the specific list acceptable for the CIS PKI is presented in Section 11.1. 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;
- Two electronic fingerprints shall be collected and stored on the card for automated authentication during card usage (See Section 11 for additional requirements);
- An electronic facial image shall be collected. The facial image shall be printed on the card and stored on the card for visual authentication during card usage. A new facial image shall be collected each time a card is issued (See Section 11 for additional requirements); and
- The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

In the event an applicant is denied a credential based on the results of the identity proofing process, the applicant shall be given an opportunity to provide additional identity documentation prior to final rejection.

For Basic Assurance Level Certificates, the applicant's identity can be verified on the basis of the declaration and/or records from the sponsoring organization, based on existing corporate or commercial data.

[3] 3REAL ID Act-compliant IDs are identified by the presence of the U.S. Department of Homeland Security REAL ID star.

For other Assurance Levels applicable to human Subscribers, identity shall be established by in-person proofing before the RA, Trusted Agent, or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy.

For Certificates asserting the medium-aero Assurance Levels, 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 identity documentation.

Requirements for authentication of individual identity using an in-person antecedent are listed in section 3.2.3.3.

3.2.3.2 Authentication of Device Identities

Some computing and communications devices (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") shall have a human sponsor (the "Device Sponsor"). The Device Sponsor shall be responsible for the security of the Private Key and for providing the following registration information:

- Equipment identification (e.g. IP address, hostname, aircraft registration number, aircraft/equipment part number) or unique software application name or service name (e.g., DNS name or function name) sufficient to uniquely identify the Subject;
- Equipment or software application Public Keys;
- Equipment or software application 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 his/her sponsorship to ensure it is still authorized 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 Sponsor shall have an established relationship with the CIS PKI.

2. The Sponsor shall have an established on-going working[4] relationship with the Applicant sufficient enough to enable the RA to, with a high degree of certainty, verify that the human Applicant is the same person that was identity proofed by the Sponsor.
3. Initial contact information for the Applicant shall be provided by the Sponsor (e.g., name, email address, phone number, etc.).
4. The Sponsor shall provide a signed statement to the RA containing the following information:
   a. Date of original identity proofing event.
   b. A description of the ID documents provided during the antecedent identity proofing process. These documents must satisfy the requirements in Section 3.2.3.1 of this C.P.
   c. Historical artefacts associated with the Antecedent event, if any.
   d. The name, date of birth, and other personal information that bind the individual to the identity.
5. Exchange of information between the Sponsor, the Applicant and the RA directly pertaining to the antecedent issuance process shall be secure, and the information shall be validated, protected, and securely exchanged.
6. The RA shall use the Applicant information provided by the Sponsor to establish contact with the Applicant.
7. The Applicant shall present a valid Sponsor-issued photo ID that matches information provided by the Sponsor as proof of identity.
8. The Applicant shall sign a declaration of identity using a handwritten signature or appropriate digital signature, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. 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[5]. 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 authorized 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 a Role Sponsor.

[4] One example of "established on-going working relationship" is the person is employed by or reports to the Certificate Sponsor. Another example is the person is a member of a professional organization which is acting as the Sponsor.

[5] Unless specifically mentioned in the text, what applies to Role Certificates also applies to Role-based Code Signing Certificates.

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 except in the case of Role Encryption Certificates used for secret protection where the encryption key pair and Role Encryption Certificate shall not be shared.

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 organization affiliation, key generation, Private Key protection, and Subscriber obligations).

For Role Signature and LSAP Code Signing Certificates:

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.

For Role Encryption Certificates:

Only the Role Sponsor may act on behalf of the Certificate subject for Certificate management activities such as:

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

PRACTICE NOTE:

When determining whether a role Certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role-based Certificates may also be used for individuals on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Chair PKI Process Action Team".

3.2.3.5 Human Subscriber Re-Authentication following loss, damage, or key compromise

If human subscriber credentials containing the Private Keys associated with the public key Certificates are lost, damaged, or stolen, the subscriber may be issued new Certificates using the process described in this section. However, the validity period of the Certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1. Alternatively, the subscriber can undergo an initial identity proofing process described in Section 3.2.3.1.

The subscriber shall present one valid National Government-issued photo ID or valid non-National Government issued photo ID (e.g., Drivers License, Passport). In addition, and where applicable, the RA shall match a good fingerprint or other adequate biometric from the subscriber with the biometric stored in an authoritative trusted database. This database shall be protected as stipulated in Section 4.3 of this CP.

The CA or an RA shall ensure that the subscriber'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. The process documentation shall include the following:

- The identity of the person performing the identity verification;
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable Certificate policy which may be met by establishing how the subscriber is known to the verifier as required by this Certificate policy;
- Unique identifying numbers from the Identifier (ID) of the verifier and from the ID of the subscriber;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature and performed in the presence of the person performing the identity authentication, using the format set forth at [28 U.S.C. 1746 -- Unsworn Declarations Under Penalty of Perjury] or comparable procedure under local law.

In addition, if the credentials are lost, stolen or otherwise unaccounted for, all Certificates associated with the Private Keys on the credentials shall be revoked for the reason of key compromise. This CP also requires that when a Certificate is revoked for the reason of key compromise, the derivative Certificates (i.e., Certificates issued on the basis of the compromised Certificate) also be revoked.

3.2.4 Non-verified Subscriber information

Subscriber information that is not verified shall not be included in Certificates.

3.2.5 Validation of authority

Prior to issuing cross-Certificates, the Issuing Carillon 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 Carillon PCA shall obtain Carillon 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.

NOTE:

Various special purpose Certificates are subject to extra requirements concerning validation of authority, as follows:

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

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

- Have a CP mapped to and determined by the Carillon 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 CA and Subscriber re-key requests shall be authenticated using their existing Private Key to sign a Subscriber request or establish a client authenticated TLS session, and validated using the associated, currently valid public key Certificate.

Alternatively, authentication shall be accomplished 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-device-software-256** **basic-hardware-256** **basic-device-hardware-256**	No further requirements
medium-softwareCBP-256 **medium-aero-software-256** **medium-software-256** **medium-hardwareCBP-256** **medium-aero-hardware-256** **medium-hardware-256** **medium-device-software-256** **medium-device-hardware-256** **IceCAP-hardware**	The initial identity-proofing process must be carried out at least once every nine (9) years

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. Alternatively, human Subscriber identity may be verified through the use of biometrics[6] retained in the IDMS as part of the original identity proofing process.

For Basic (or lower) Assurance Level Certificates, in case of loss, theft or malfunction the new registration process could consider some of the previously provided subscriber information, as still valid (e.g. General Terms and Conditions). Nevertheless, the

[6] Fingerprints may be used for this purpose, facial image may not.

registration authority shall perform the same controls as during the initial registration process.

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.

Other revocation request authentication mechanisms may be used as well, as long as they include an authentication method commensurate with the Assurance Level of the Certificate whose revocation is being requested.

All revocation requests shall be logged.

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 TLS Certificate issued under medium-software policy and set up with appropriate algorithms and key sizes satisfies integrity and confidentiality requirements for medium-software Certificate management.

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

Certificates and corresponding Private Keys must be managed safely at their initial creation through their full life-cycle.

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

For all Assurance Levels applicable to non-human Subscribers, 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 CA-Certificate applications to a Carillon Root or PCA, an authorised representative of the Subject CA shall submit the application to the Carillon PMA.

4.1.2 Enrolment process and responsibilities

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

All communications supporting the Certificate application and issuance process shall be authenticated and protected from modification. Cryptographic mechanisms commensurate with the strength of the Private Key shall be used to protect electronic communications between the RA and CA.

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 Carillon PMA shall verify all authorisations and other attribute information received from an applicant CA.

All Subscribers must agree to be bound by a relevant Subscriber Agreement that contains representations and warranties described in 9.6.2.

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;
- 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 Carillon PMA shall establish its criteria and procedures describing how other entities may apply for and receive a Cross-certificate and how Sub CAs may apply for and receive a Certificate from a Carillon Root or PCA.

A Carillon Root CA shall certify Carillon Sub CAs implementing this CP only as authorised by the Carillon 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 Carillon Sub CA.

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

The Carillon 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[7].

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

Carillon CAs shall only issue Certificates asserting the OIDs outlined in this CP upon receipt of written authorisation from the Carillon PMA, and then may only do so within the constraints imposed by the Carillon 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 Carillon 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 contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized 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

RAs must ensure that the identification and authentication measures listed in section 3 are applied.

4.2.2 Approval or rejection of Certificate applications

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

For CAs the Carillon PMA may approve or reject a Certificate application.

A Certificate application shall be approved if all of the following conditions are met:

- successful identification and authentication of all required Subscriber information as described in 3.2.3; and
- payment (if applicable) has been received.

A Certificate application shall be rejected if any one or more of the following conditions arises:

- identification and authentication of all required Subscriber information as described in section 3.2.3 cannot be completed;

[7] Note that subordinated CAs (Carillon Sub CAs) inheriting this CP do not require policy mapping.

- the Subscriber fails to furnish supporting documentation upon request;
- the Subscriber fails to respond to notices within a specified time;
- payment (if applicable) has not been received; or
- the RA or CA believe that issuing a Certificate to the Subscriber may bring the CA into disrepute.

IceCAP-hardware Certificates shall only be issued to human Subscribers.

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.

For levels of assurance Medium and above, when information is obtained through one or more data sources, the CA shall ensure there is an auditable chain of custody.

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:

- verify the identity and authority of the requestor,
- verify the information in the request before inclusion in the Certificate,
- ensure that the Public Key is bound to the correct Subscriber,
- obtain a proof of possession of the Private Key,
- generate and sign the Certificate,
- provide the Certificate to the Subscriber,
- when applicable, publish the Certificate to the repository as described in section 2 of this CP and in the applicable CPS, after formal Subscriber acceptance.

Certificates shall be checked to ensure that all fields and extensions are properly populated.

If databases are trusted to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the Certificate being sought. Specifically, the databases shall be protected using physical security, personnel controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

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

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

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

4.4 Certificate Acceptance

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. End-Entity Subscribers shall accept the responsibilities defined in Section 9.6.3 by signing the Subscriber Agreement during Certificate issuance.

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

Carillon 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.

4.4.2 Publication of the Certificate by the CA

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

Subscriber Certificates containing the IceCAP-hardware and IceCAP-cardAuth policy OIDs shall not be published in a public repository.

4.4.3 Notification of Certificate issuance by the CA to other entities

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

The Carillon 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 Carillon CAs and to cross-certified PKI domains' PMAs according to the contractual obligations established through the respective MOA by the Carillon PMA. In addition, the new CA Certificates shall be provided to the cross-certified PKI domain's PMA.

A Carillon PCA is not cross-certified with more than one external PKI domain CA.

In the event a CA renews, re-keys or modifies a Certificate without interaction with the RA system involved in the existing Certificate's issuance, the CA must notify the RA of the action taken.

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.

Subscribers and CAs shall discontinue use of the Private Key upon expiration or revocation of the Certificate, except for decryption purposes.

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 should obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties should 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, as described in RFC 5280, including revocation status according to section 4.9.6.

Assuming that the use of the Certificate is appropriate, Relying Parties should 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.

In cryptographic systems where usage of a Time Stamping service is expected by the Relying Party, in addition to all other verifications stated in this section, Relying Parties verifying software packages should perform at least the following checks:

- verify the validity of all the Certificates, including the Time Stamp Authority's

Certificate, and their trust chains, following the requirements of RFC 5280;

- verify that the timestamp is compliant with RFC 3161;
- verify that the timestamp applies to all the PKI objects in the package. The PKI objects shall be used to build and verify the certification path for the signer as of the time of the timestamp;
- verify that the timestamp was issued by a recognised Time Stamping Authority. This shall be checked by building a path to a trust anchor, ensuring that the trust anchor is permitted for timestamp Certificate purposes, and ensuring that the Time Stamping Authority's Certificate contains the appropriate EKU OID;
- verify that the timestamp shows a time that predates the time at which the check takes place; and
- verify that the timestamp shows a time that predates the "notAfter" date of the Certificate used to digitally sign the software package.

4.6 Certificate Renewal

Renewing a Certificate means creating a new Certificate with a new serial number where all Certificate subject information , including subject public key, and subject key identifier, remain unchanged. The new Certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, different AIA and/or be signed with a different issuer key).

After Certificate renewal, the old Certificate may or may not be revoked, but must not be used for requesting further renewals, re-keys, , or modifications.

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 it has not reached the end of its validity period or been revoked, the associated Private Key has not been compromised, and the Subscriber name and attributes are unchanged. 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.

Subscriber Certificates containing an IceCAP policy OID shall not be renewed, except during recovery from CA key compromise. In such cases, the renewed Certificate shall expire as specified in the original Subscriber Certificate.

CA Certificates and delegated OCSP responder Certificates may be renewed so long as the aggregated lifetime of the Private Key does not exceed the requirements specified in Section 5.6.

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.

An RA may request renewal of a Subscriber 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 a Carillon PCA, Certificate renewal also requires that a valid MOA exists between the Carillon PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new Certificate.

When Certificates are renewed as a result of CA key compromise, the CA or RA must verify all Certificates issued since the date of compromise were issued appropriately. If the Certificate cannot be verified, it must not be renewed.

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

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 may or may not be revoked, but shall not be used for requesting further re-keys, renewals, or modifications.

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 re-key of Role Signature, Role Encryption and LSAP Code Signing Certificates for which he/she is the sponsor.

The individual identified in a Role Signature Certificate may request re-key of his/her Role Signature Certificate

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

An external PKI domain's PMA may request re-key of its cross 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 Carillon 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, Role Encryption, and LSAP Code Signing 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

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that differs in one or more other fields, from an existing, currently valid Certificate. For example, a Carillon Sub CA may choose to update a Certificate of a Subscriber whose characteristics have changed (e.g., has been assigned a new email address). The old Certificate may or may not be revoked, but must not be used for further modifications, re-keys, or renewals.

Certificate modification is only supported by this CP for CA Certificates, CIV-contentSigning and IceCAP-contentSigning 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, e.g., change in subject attributes, etc., and the Subject continues to be entitled to a Certificate.

4.8.2 Who may request Certificate modification

The PMA may request modification of a Carillon CA Certificate.

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

The OA may request modification of an IceCAP-contentSigning or a CIV-contentSigning 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.

In the event the modified Certificate indicates a reduction in assurance level, the old Certificate must be revoked.

For Cross-Certificates issued by a Carillon 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; the CA shall ensure in its agreements with a Subscriber's Affiliated Organisations that the Organisation be required to notify the CA of any changes to the Subscriber's affiliation.
- An organization 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 its 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 his/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. Revoked Certificates shall appear on at least one CRL.

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 authorized by directly or indirectly chaining back to that compromised key shall be revoked.

Carillon PKI shall request that the cross-certified entity revoke its Cross-Certificate if it does not meet the stipulations of the Certificate policies listed in the Cross-Certificate, including the relevant policy OIDs and "pass-through" policy OIDs.

The Carillon PKI shall notify the cross-certified entity at least two (2) weeks and one day prior to the revocation of a CA Certificate, whenever possible. In the case of an emergency CA Certificate revocation, the notification procedures from section 5.7 shall be followed.

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 device they have sponsored, issuing CA, or RA may request revocation of a Certificate.

For Role Signature Certificates and for LSAP Code Signing 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 a Carillon PCA, the external PKI domain PMA or the Carillon 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, a Carillon 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 Carillon 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 a Carillon Root or PCA, the Operational Authority shall seek guidance from the Carillon PMA before revocation of the Certificate except when the Carillon 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 Carillon PKI.

For Certificates issued by a Carillon Sub 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 Carillon 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. For IceCAP Certificates, Certificate revocation is mandatory regardless of whether the hardware token is retrieved and zeroized or destroyed.

If a Subscriber's token is lost or stolen, then all Subscriber Certificates associated with that token shall be revoked immediately 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

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

For Carillon Sub CAs, processing time for Subscriber Certificate revocation requests is specified below:

Assurance Level	Processing Time for Revocation Requests
basic-software-256 basic-device-software-256 basic-hardware-256 basic-device-hardware-256	Within twenty-four (24) hours of receipt of request
medium-softwareCBP-256 medium-aero-software-256 medium-software-256 medium-device-software-256 medium-hardwareCBP-256 medium-aero-hardware-256 medium-hardware-256 medium-device-hardware-256 IceCAP-hardware IceCAP-cardAuth IceCAP-contentSigning	Before next CRL is generated unless request is received within 2 hours of scheduled CRL generation, in which case revocation requests must be processed before the following scheduled 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.

PRACTICE NOTE:

In the cases where the CRL issued by the CA has a validity period

longer than 24 hours, the Relying Party should check for a refreshed CRL every 24 hours to obtain the latest Cross-Certificate revocations reported

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 offline 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 monthly. At least once every eighteen (18) 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 Carillon 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.

The CRLs for online CAs shall be published within 4 hours of generation.

For offline CAs, pre-generated CRLs intended for publication more than 4 hours after generation shall be protected in a manner commensurate with the protection of the CA until publication. Existing unpublished CRLs must be securely destroyed in the event the CA revokes a Certificate.

The CA shall coordinate with repositories to reduce the latency between the moment the CA desires the CRL to be published and the moment the CRL is available to Relying Parties within the applicable repositories.

4.9.9 On-line revocation/status checking availability

For IceCAP Certificates, Carillon CAs shall support on-line status checking via OCSP using the CA-delegated trust model [RFC 6960]. For other types of Certificates, the Carillon CAs are not required to operate an OCSP Responder covering the Certificates they issue.

The Carillon PKI Repository shall contain and publish a list of all OCSP Responders operated by the Carillon CAs.

If OCSP is implemented, the service shall comply with the Internet Engineering Task Force (IETF) RFC 6960 to meet security and interoperability requirements.

In addition to CRLs, CAs and Relying Party client software may 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

Relying Parties are not required to utilize OCSP. If a Relying Party relies on OCSP, it should do so in accordance with the requirements in RFC 6960.

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; and

- the alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

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".

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 Carillon PKI is required to provide Online Certificate Status Protocol (OCSP) services for the IceCAP Assurance Level Certificates it issues.

4.10.1 Operational characteristics

The Carillon PKI OCSP service shall be described in the Sub CA CPS.

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.

Certificate Status Services, where implemented, shall be available on a 24x7 basis, with a minimum of 99.9% availability overall per year and a scheduled downtime not to exceed 0.5% annually.

The Carillon PKI OCSP service shall be described in the Sub CA CPS.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

A Subscriber may terminate his subscription either by allowing his Certificate to expire without renewing or re-keying it, or by revoking his Certificate before expiry without applying for a replacement.

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.

For Carillon CAs that escrow the private keys of encryption Certificates at Medium or higher Assurance Levels, a Key Recovery Practise Statement ([KRPS]) shall be developed. The [KRPS] shall be validated by an auditor designated by the PMA of external PKI domains Cross-Certified at the appropriate Assurance Levels to be in compliance with the appropriate Key Recovery Policy (KRP). The Carillon PMA shall ensure that the PKI operates in compliance with the [KRPS] for encryption Certificates at Medium or higher Assurance Levels.

For Carillon CAs that escrow the private keys of encryption Certificates at Basic or lower Assurance Levels only, the following requirements must be met:

- the Key Escrow System must be operated under the same facility, management and operational controls as the CA, as described in section 5 of this CP
- the Key Escrow System must be operated under the same technical security controls as the CA, as described in section 6 of this CP
- during all steps of its storage or recovery, an escrowed private decryption key must be encrypted with a symmetric or public key of a cryptographic strength equivalent or superior to the escrowed private decryption key

- recovery of a Subscriber's escrowed private decryption keys shall only be requested by one of the following:
    - the Card Management System during card issuance for that Subscriber
    - the Subscriber or its Device Sponsor, authenticated as described in section 3 of this CP.

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, CMS, and STP 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, CMS, and STP equipment and records.

Administration Workstations used to administer CA, CSA, CMS, and/or STP 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, CMS, and STP 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, CMS, STP 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 offline 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 Carillon standard data centre procedures. CA, CSA, CMS, STP, RA and Administration Workstation 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

CA, CSA, CMS, STP, RA, and Administration Workstation equipment shall be installed such that the possibility of fire is minimized. Operational environment shall be equipped with temperature and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment. Operating material (e.g., software, keys) shall be stored such that

they are protected from fire.

5.1.6 Media storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic), theft and unauthorized 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 offline, 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.

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 CPSs;

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

The individuals assigned to CA trusted roles also may be assigned to the corresponding CSA trusted roles identified above (i.e., a CA Administrator may also fulfil the CSA Administrator role, a CA Audit Administrator may also fulfil the CSA Audit Administrator role).

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 Administrators 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 Administrators 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 CPSs.

The CMS Operators shall be responsible for:

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

The individuals assigned to CA trusted roles also may be assigned to the corresponding CMS trusted roles identified above (i.e., a CA Administrator may also fulfil the CMS Administrator role, a CA Audit Administrator may also fulfil the CMS Audit Administrator role).

5.2.1.7 STP Roles

An STP 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 STP Administrator shall be responsible for:

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

The STP Audit Administrator shall be responsible for:

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

The STP Operator shall be responsible for:

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

The individuals assigned to CA trusted roles also may be assigned to the corresponding STP trusted roles identified above (i.e., a CA Administrator may also fulfil the STP Administrator role, a CA Audit Administrator may also fulfil the STP Audit Administrator role).

5.2.2 Number of persons required per task

The following tasks shall require two (2) or more persons serving in a trusted role, as defined in section 5.2.1, at least one of which shall be an Administrator:

- CA, CSA, CIV content Signing and IceCAP content Signing key generation;
- CA, CSA, CIV content Signing and IceCAP content Signing key activation; and
- CA, CSA, CIV content Signing and IceCAP content Signing Private Key backup.

The following task shall require two (2) or more persons, at least one of which shall be a Registration Authority:

- IceCAP-cardAuth Certificate issuance.

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 to 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 which manages PIV-I cards shall be allowed access only when authenticated using a method commensurate with IceCAP-hardware 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, CMS, and STP 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 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, CMS, and STP 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 a favorable outcome from the background investigation;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their duties for the trusted role; and

- Be appointed in writing by an approving authority.

In addition, the person filling the trusted role shall not knowingly:

- Have been previously relieved of duties resulting from violation of trust (e.g., willful mishandling of information or willful mis-issuance of a Certificate);
- Have had a security clearance revoked for reasons other than routine review and renewal decisions;
- Have been denied a security clearance, the cause for which has not been resolved and a security clearance subsequently granted; and
- Have been criminally convicted as legally reportable (e.g., felony offense, serious crime).

For CAs issuing Certificates at Medium (or higher) Assurance Levels (excluding CAs operating only at the CBP Assurance Levels), each person filling a trusted role shall satisfy at least one of the following requirements:

- 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; or
- The person 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.

5.3.2 Background check procedures

All persons filling CA trusted roles, CSA trusted roles, CMS trusted roles, STP trusted roles, and RA roles shall have completed a background investigation as allowed by applicable national law or regulation. The scope of the investigation shall include checking 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 (for past 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.

A favorable national agency check or security clearance that is based on a five-year background investigation meets the requirements of this section. For example, a

successfully adjudicated United States National Agency Check with Written Inquires (NACI) or United States National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the requirements of this section, as is a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by ITAR – 22 CFR 120.32.

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

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, STP, or individuals performing Trusted Agent or RA roles shall receive comprehensive training.

Training shall be conducted in the following areas:

- CA/CSA/CMS/STP/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
- Stipulations of the applicable CP and CPS

A record of the training completed for each individual shall be maintained by the organization administering the CA.

5.3.4 Retraining frequency and requirements

Individuals responsible for trusted roles shall be aware of changes in the CA, CSA, CMS, STP, 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

Job rotation is optional. Any job rotation shall ensure the following:

- Role separation requirements are not violated,
- The continuity and integrity of the CA services are not affected,
- All access rights associated with the previous role(s) are terminated,
- A record of each role change is maintained, and
- Individuals assuming an auditor role do not audit their own work from a previous role.

5.3.6 Sanctions for unauthorised actions

The Carillon Information Security Inc. 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

Sub-Contractor personnel employed to perform functions pertaining to CA, CSA, CMS, STP, 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 CP, CPS, and any relevant complementary documents, such as statutes, policies and contracts, shall be made available to all trusted role personnel. 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.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSAs, CMSes, STPs, RAs, and Administration Workstations. 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 5.4.3.

A statistically significant sample of security audit data since the last review shall be examined to include a reasonable search for any evidence of malicious activity. Where possible, audit record reviews should be performed using an automated process. 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. In addition, the event log of the Administration Workstation shall be reconciled with the event log of the corresponding CA, CMS, CSA, STP, or RA. The Audit Administrator shall explain all significant events in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.1 Types of events recorded

All security auditing capabilities of the CA, CSA, CMS, STP, Administration Workstations, and RA operating system and the CA, CSA, CMS, STP, 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,
- Location of the event (system affected or physical locations),
- Source of the event,

- Success or failure where appropriate, and
- The identity of any entity, object, and/or operator associated with the event.

Any request or action requiring the use of a private key controlled by the CA is an auditable event. If out-of-band processes are used for authorization of Certificate issuance, external artefacts from the process (e.g., forms, emails, etc.) must be recorded.

The following events shall be audited[8]:

Auditable Event	CA	CSA	RA	CMS	STP	AW
SECURITY AUDIT						
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X	X	X
IDENTITY-PROOFING						
Platform or CA application-level authentication attempts	X	X	X	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X	X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login	X	X	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	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	X
DATA ENTRY AND OUTPUT						
Any additional event that is relevant to the security of the CA (e.g., remote or local data entry or data export) must be documented	X	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	X
PRIVATE KEY LOAD AND STORAGE						

[8] 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.

Auditable Event	CA	CSA	RA	CMS	STP	AW
The loading of Component Private Keys	X	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	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	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	X
CERTIFICATE REGISTRATION						
All records related to Certificate request authorization, approval and signature	X	N/A	X	X	X	N/A
CERTIFICATE REVOCATION						
All records related to Certificate revocation request authorization, approval and execution	X	N/A	X	X	X	N/A
CERTIFICATE STATUS CHANGE APPROVAL						
All records related to Certificate status change request authorization, approval and execution	X	N/A	N/A	X	X	N/A
PKI COMPONENT CONFIGURATION						
Any security-relevant changes to the configuration of the Component	X	X	X	X	X	X
ACCOUNT ADMINISTRATION						
Roles and users are added or deleted	X	N/A	N/A	X	X	X
The access control privileges of a user account or a role are modified	X	N/A	N/A	X	X	X
CERTIFICATE PROFILE MANAGEMENT						
All changes to the Certificate profile	X	N/A	N/A	X	N/A	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	N/A
REVOCATION PROFILE MANAGEMENT						
All changes to the revocation profile	X	N/A	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT						

Auditable Event	CA	CSA	RA	CMS	STP	AW
All changes to the Certificate revocation list profile	X	N/A	N/A	N/A	N/A	N/A
MISCELLANEOUS						
Appointment of an individual to a Trusted Role or removal from the Trusted Role, including a record of who added or removed them from the role	X	X	X	X	X	X
Designation of personnel for multiparty control	X	N/A	N/A	X	X	X
Installation of the Operating System	X	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	X	N/A
Installation of hardware cryptographic modules	X	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X	X
System Start-up	X	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X	X
Back up of the internal CA database	X	N/A	N/A	X	X	N/A
Restoration from back up of the internal CA database	X	N/A	N/A	X	N/A	N/A
Critical file manipulation (e.g., creation, renaming, moving)	X	N/A	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	N/A
Access to the internal CA database	X	X	N/A	N/A	N/A	N/A
All Certificate compromise notification requests	X	N/A	X	X	N/A	N/A
Loading tokens with Certificates	X	N/A	X	X	X	N/A
Shipment of Tokens and receipt of Tokens from/by the component that contain key material or that allow access to key material	X	N/A	X	X	N/A	N/A
Zeroising Tokens	X	N/A	X	X	N/A	N/A
Re-key of the Component	X[9]	X	X	X	X	X
CONFIGURATION CHANGES						
Hardware	X	X	N/A	X	X	X

[9] While this CP prohibits re-key of a Carillon PKI CA, the audit control should still record any attempt to re-key the CA.

Auditable Event	CA	CSA	RA	CMS	STP	AW
Software	X	X	X	X	X	X
Operating System	X	X	X	X	X	X
Patches	X	X	N/A	X	X	X
Security Profiles	X	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY						
Personnel Access to room housing Component	X	N/A	N/A	X	X	X
Access to the Component	X	X	N/A	X	X	X
Known or suspected violations of physical security	X	X	X	X	X	X
ANOMALIES						
Software error conditions	X	X	X	X	X	X
Software check integrity failures	X	X	X	X	X	X
Equipment failure	X	N/A	N/A	X	X	N/A
Electrical power outages	X	N/A	N/A	X	X	N/A
Uninterruptible Power Supply (UPS) failure	X	N/A	N/A	X	X	N/A
Obvious and significant network service or access failures	X	N/A	N/A	X	X	N/A
Violations of Certificate Policy	X	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X	X

5.4.2 Frequency of processing log

Audit logs shall be reviewed at least monthly, 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.

5.4.3 Retention period for audit log

Audit logs shall be retained onsite for at least sixty (60) days or until they are reviewed, whichever come later.

5.4.4 Protection of audit log

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

- Only authorised people shall have read access to the audit logs;
- Only authorised people may archive audit logs; and,
- Audit logs shall not be modified.

For the CA, CMS, CSA, STP, and the Administration Workstations, the only authorised individual shall be the Audit Administrator. For an RA, the authorised individual shall be a system administrator other than the RA.

Procedures must be implemented to protect audit records from unauthorized deletion or destruction.

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 monthly 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, STP, or RA. Audit processes shall be invoked at system start-up and cease only at system shutdown. Audit collection systems shall be configured to ensure security audit data is protected against loss (e.g., overwriting or overflow of automated log files). If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem is remedied.

5.4.7 Notification to event-causing subject

There is 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

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 shall be performed at least monthly.

5.5 Records Archival

5.5.1 Types of records archived

CA, CSA, CMS, STP, 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, CSA, or STP 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	STP
Certification Practice Statement	X/X	X	X	X	X
Certificate Policy	X	X	X	X	X
Contractual obligations	X/X	X	X	X	X
Other agreements concerning operations of the CA	X/X	X	X	X	X
System and equipment configuration	X/X	X	-	X	X
Modifications and updates to system or configuration	X/X	X	-	X	X
All records related to Certificate request, authorization, approval and signature	X/X	-	-	X	N/A
All records related to Certificate revocation	X/X	-	-	X	N/A
Subscriber identity authentication data as per section 3.2.3	N/A / X	N/A	X	X	N/A
Documentation of receipt and acceptance of Certificates, including Subscriber Agreements	X/X	N/A	X	X	N/A
Documentation of receipt of Tokens	N/A / X	N/A	X	X	N/A
All Certificates issued or published	X/X	N/A	N/A	X	N/A
Record of Component CA Re-key	N/A / N/A	X	X	X	X
All CRLs and CRLs issued and/or published	X/X	N/A	N/A	N/A	N/A
All Audit Logs	X/X	X	X	X	X
Other data or applications to verify archive contents	X/X	X	X	X	X
Documentation required by compliance auditors	X/X	X	X	X	X
Compliance Audit Reports	X	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. The archive retention period for records associated with a specific CA begins at CA key generation and shall be maintained for a minimum of three (3) years following CA expiration or termination. 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 processing the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of archive

The archive must be protected as specified by the privacy laws of the country where the Subscriber information was collected.

Only authorized individuals shall be permitted to write to, modify, or delete the archive. For the CA, CSA, CMS, and STP, 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 Carillon PMA for the Carillon 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, STP, 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. Deletion of archive records is not permitted under any circumstances prior to the end of the required retention period.

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 have accurate timestamps with sufficient precision such that the sequence of events can be determined. 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)

An archive collection system shall be in place, and shall be described in the CPS.

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.

The contents of the archive shall not be released except in accordance with Sections 9.3 and 9.4.

5.6 Key Changeover

As a CA approaches the end of its validity period, planning should be put in place to ensure a smooth transition to a new CA, unless it is the intention of the organization to cease Certificate production. Prior to the end of a CA private key's signing validity period, a new CA shall be established.

Once a new CA has been established, 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. The old Private Key shall continue to be used to sign CRLs and OCSP Responder Certificates until the expiration of the CA Certificate or expiration/revocation of all Certificates issued by the CA, whichever comes first, and must be protected accordingly. The key changeover processes shall be described in the applicable CPS.

The following table provides the maximum lifetimes for Certificates and associated Private Keys.

Key	2048 Bits		4096 Bit Keys	
	Private Key	**Certificate**	**Private Key**	**Certificate**
Carillon Root CAs	20 years	20 years	20 years	20 years
Carillon Sub CAs	5 years	≤ 10 years	10 years	≤ 13 years[10]
Subscriber Identity or Signature	3 years	≤ 3 years	3 years	≤ 3 years
Subscriber Encryption	Unrestricted	≤ 3 years	Unrestricted	≤ 3 years
Role Identity	3 years	≤ 3 years	3 years	≤ 3 years
Role Signature	3 years	≤ 3 years	3 years	≤ 3 years
Role Encryption	Unrestricted	≤ 3 years	Unrestricted	≤ 3 years
LSAP Code Signing	3 years	≤ 8 years	3 years	≤ 8 years
Code Signing or Role-Based Code Signing	≤3 years	≤ 8 years	≤3 years	≤ 8 years
CIV Content Signer	3 years	≤ 9 years	3 years	≤ 9 years
IceCAP Content Signer	3 years	≤ 9 years	3 years	≤ 9 years
Server or Device Identity or Signature	3 years	≤ 3 years	3 years	≤ 3 years
Server or Device	Unrestricted	≤ 3 years	Unrestricted	≤ 3 years

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

Encryption				
OCSP Responders	≤ 3 years	≤ 120 days	≤ 3 years	≤ 120 days
SCVP Servers	≤ 1 year or 500 000 signatures	≤ 3 years	≤ 1 year or 500 000 signatures	≤ 3 years
TSA signed by Root CA	≤ 1 year or 500 000 signatures	≤20 years	≤ 1 year or 500 000 signatures	≤20 years
TSA signed by Signing CA	≤ 1 year or 500 000 signatures	≤10 years	≤ 1 year or 500 000 signatures	≤13 years

CIV-cardAuth, IceCAP-hardware and IceCAP-cardAuth Certificate expiration shall not be later than the expiration date of the hardware token on which the Certificates reside.

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.

For additional constraints on Certificate life and key sizes, see Section 6.1.5.

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 Carillon PKI Domain.

If a CA, CSA, or STP 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, CSA, or STP 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, CSA, or STP needs to be rebuilt, only some Certificates need to be revoked, and/or the CA, CSA, or STP key needs to be declared compromised. If it is determined that an incident has occurred with the potential to affect the operations and/or security environments, all cross-certified entities shall be notified within 24 hours of determination and provided a preliminary remediation analysis.

Once the incident has been resolved, the OA shall notify all cross-certified entities. The notification shall provide detailed measures taken to remediate the incident and include the following:

- Which CA components were affected by the incident;
- The CA's interpretation of the incident;
- Who is impacted by the incident;
- When the incident was discovered; and
- A statement that the incident has been fully remediated.

The Carillon PMA members and other cross-certified entities shall be notified within 24 hours of determination if any of the following cases occur:

- suspected or detected compromise of a Carillon CA system;
- physical or electronic attempts to penetrate a Carillon CA system;
- denial of service attacks on a Carillon CA component;
- any incident preventing a Carillon 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 OA shall follow the process identified above to notify all cross-certified entities of the final incident resolution.

If the STP is compromised or suspected of being compromised, the incident must be investigated. All Certificates associated with the Subscriber private keys held in the STP must be revoked within 48 hours unless a definitive determination is made that the STP is not compromised.

The Carillon PMA members and other domain PKI (who entered a MOA with Carillon) 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 time-frame, 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 Private Key compromise procedures

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

1. The CA shall request revocation of any Certificates issued to the compromised CA immediately;
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 a Carillon Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The Carillon 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 Carillon 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 a CMS IceCAP-contentSigning or CMS CIV-contentSigning signature key is compromised or lost (such that compromise is possible, even though not certain), the CMS shall follow the applicable procedures in Section 5.7.1.

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 re-establish operations as quickly as possible by following 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.

Any issued Certificates that have not expired shall be revoked, and a final long-term CRL with a nextUpdate time past the validity period of all issued Certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued Certificates has passed. Once the last CRL has been issued, the private signing key(s) of the terminated CA shall be destroyed.

In the event of a Carillon Root CA or Carillon Sub CA termination, cross-certified PKIs will be notified at least two (2) weeks and one day prior to termination, if circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

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

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

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

If a Carillon Root CA is terminated, that Carillon Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated Carillon 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[11]
  - 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 Level	Hardware or Software	Key Storage Restricted to the Module on which the Key was Generated
CA	3	Hardware	Yes
CMS	2[12]	Hardware	Yes
RA	2	Hardware	Yes
OCSP Responder	2	Hardware	Yes
SCVP Server	3	Hardware	Yes
TSA	3	Hardware	Yes
STP	3	Hardware	Yes
LSAP Code Signing	2	Hardware	Yes
Code Signing	2	Hardware	Yes
Role-Based Code Signing	2	Hardware	Yes
basic-software-256 **basic-device-software-256**	1[13]	Software	No requirements
basic-hardware-256 **basic-device hardware-256**	No requirements	Hardware	No requirements
medium-softwareCBP-256 **medium-aero-software-256**	1[13]	Software	No requirements

[11] 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.

[12] If a CMS is also used as a Key Server (see *CertiPath KRP*), the FIPS 140 requirement becomes Level 3 due to the constraints imposed on Key Servers.

[13] An equivalent certification delivered by a national or international standards body, as approved by the PMA, may be used instead of the FIPS certification. The certification may apply to a previous version of the software security module, antecedent to the version in use.

medium-software-256 **medium-device-software-256**			
medium-hardwareCBP-256 **medium-aero-hardware-256** **medium-hardware-256** **medium-device-hardware-256**	2[14]	Hardware	Yes
IceCAP-hardware	2 (section 11 also applies)	Hardware	Yes
CIV-cardAuth	No requirements	Hardware	No requirements
CIV-contentSigning	No requirements	Hardware	No requirements
IceCAP-cardAuth	2 (section 11 also applies)	Hardware	Yes
IceCAP-contentSigning	2	Hardware	Yes

Key generation must be performed using a method validated against FIPS 140 or an equivalent international standard. Key generation events should use the configuration that was the basis of the validation (e.g., FIPS-validated modules should be operated in FIPS mode). If the required keys cannot be generated while in a validated configuration, the specific configuration and reason for use of a different method should be documented by the CA.

Random numbers for medium-hardwareCBP-256, medium-aero-hardware-256, medium-hardware-256, medium-device-hardware-256, and all IceCAP Assurance Level Subscriber keys shall be generated in FIPS 140 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 IceCAP-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

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

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:

- 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 Subscriber Key Pair.

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:

- Secure distribution of a trust anchor through secure out-of-band mechanisms; or
- Downloading a trust anchor from a web site secured with a currently valid Certificate and subsequent comparison of the hash of the Certificate against a hash value 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).

6.1.5 Key sizes

If the Carillon 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 Carillon CAs to revoke the affected Certificates, according to the applicable MOA.

All public keys placed in newly generated Certificates (including self-signed Certificates) and uses of public key cryptography by PKI components for signature and/or key agreement/encryption operations shall use the following algorithm suites for the time periods indicated:

	Public Key Algorithm	Sunset Date
Signature	2048 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field	12/31/2030
	3072 or 4096 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field	No stipulation
Encryption	2048 bit RSA, 256 bit ECDH in prime field, or 283 bit ECDH in binary field	12/31/2030
	3072 or 4096 bit RSA, 256 bit ECDH in prime field, or 283 bit ECDH in binary field	No stipulation

All data encryption (including network protocols) used by or in connection with PKI components for administration, communications, and protection of keys or other sensitive data shall use the following symmetric algorithms for the time periods indicated:

Symmetric Algorithm	Sunset Date
3 Key TDES	Deprecated. May be used until 12/31/2023 only for data blocks that are 8 MB or less per unique key bundle. [15]
AES	No stipulation

[15] See NIST SP 800-131 regarding the deprecation of 3 Key TDES

All CAs shall use 2048 bit RSA, or 256 bit prime field or 283 bit binary field, or stronger.

All CAs shall use SHA-256 or stronger, and shall not use SHA-1 in their 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.

All PKI components that use hash algorithms for security relevant functions, such as key generation or agreement, communication protocols (e.g. TLS), or password protection, shall use the same or larger bit versions of the hash algorithm(s) used by the CA to sign Certificates.

All IceCAP Certificates shall contain public keys and algorithms that also conform to [NIST SP 800-78].

Certificates asserting the IceCAP assurance levels, and the "-256" assurance levels shall only be signed using SHA256.

6.1.6 Public key parameters generation and quality checking

For RSA the PKI shall conduct Public Key parameters generation and quality checking in accordance with NIST SP 800-89[16].

For ECC, Public Keys shall fall within curves defined in Section 7.1.3. Additionally, the PKI shall confirm the validity of all keys as specified in NIST SP 800-56A.

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 Carillon CAs. This includes, but is not limited to, the following examples:

- Certificates to be used for authentication shall only set the digitalSignature bit;
- Certificates to be used by Human Subscribers for Digital Signatures shall set the digitalSignature and nonRepudiation bits;
- Certificates that have the nonRepudiation bit set, shall not have keyEncipherment bit 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;
- IceCAP-contentSigning Certificates shall include an extended key usage of id-fpki-pivi-content-signing; and
- CA Certificates shall include cRLSign and keyCertSign bits.

Keys associated with CA Certificates shall be used for signing Certificates and CRLs only.

[16] For Basic Assurance Levels, an equivalent national or international standard, as approved by the PMA, may be used instead of the FIPS standard.

Public keys that are bound into Human Subscriber Certificates shall be certified for use in signing or encrypting, but not both.

Device Subscriber Certificates 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) may set both.

With the exception of OCSP Responder, SCVP Server and TSA Certificates, Device Certificates must not assert the nonRepudiation bit.

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 values shall be consistent with key usage bits asserted.

Code signed using a Certificate asserting the nonRepudiation keyUsage shall be accompanied by an RFC 3161-compliant timestamp.

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 140, "Security Requirements for Cryptographic Modules". The Carillon PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Carillon PMA. Cryptographic modules shall be validated to the FIPS 140 level identified in section 6.1.1, or equivalent. Additionally, the Carillon 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 shall not exist outside of their cryptographic modules in plaintext form.

For IceCAP-hardware tokens, refer to section 11.

6.2.1.1 Signature Trust Platform Key Stores

Signature Trust Platform (STP) Key Stores hold keys for a number of Subscriber Certificates in one location. When a collection of private keys for Subscriber Certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber; therefore, STP Key Stores shall utilize a minimum FIPS 140 Level 3 or equivalent cryptographic module for key storage.

The STP shall be deployed so as to provide 99% availability.

Authentication to the STP in order to activate the private key associated with a given Certificate requires multi-factor authentication commensurate with the assurance level of the Certificate.

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

Use of a CA private signing key, CSA private signing key, CIV-contentSigning Private Key or an IceCAP-contentSigning Private Key shall require action by at least two (2) persons.

6.2.3 Private Key escrow

Under no circumstances shall any signature key be escrowed.

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 roles, where the encrypted data will not need to be recovered;
- decryption Private Keys associated with aircraft and/or aircraft equipment encryption Certificates which do not need to be escrowed; and
- decryption Private Keys associated with devices, where the encrypted data will not need to be recovered.

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 the one 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 asserting basic-software-256, medium-aero-software-256, medium-software-256, and/or medium-softwareCBP-256 may be backed up or copied but the backup 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 an Assurance Level other than those listed above for human Subscriber shall not be backed up or copied.

Subscriber private keys held in an STP may be backed up to a device providing comparable protection levels and approved for STP use. The STP backup shall be performed under two-person control.

Device private signature keys whose corresponding Public Key is contained in a Certificate asserting medium-software Assurance Levels and/or lower 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.

Device signature keys whose corresponding Public Key is contained in a Certificate asserting medium-hardware Assurance Levels and/or higher shall not be backed up or copied.

6.2.4.3 Backup of Subscriber Decryption Private Keys

Backed up Subscriber decryption private keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.4.4 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. An additional backup copy, if made, shall be kept under the same conditions at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.4.5 IceCAP and CIV Content Signing Key Backup

If backed up, the IceCAP-contentSigning and CIV-contentSigning private keys shall be backed up under the same multi-person control as used to generate the original Content Signing key.

When implemented, procedures for IceCAP-contentSigning and CIV-contentSigning Private Key backup and storage shall be included in the appropriate CPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.4.6 Backup of STP Private Keys

STP private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

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 private decryption 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 a Carillon Key Recovery Practise Statement (KRPS).

6.2.6 Private Key transfer into or from a cryptographic module

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

The Private Keys may be backed up in accordance with section 6.2.4.

If any private key is transported from one cryptographic module to another, the Private

Key shall be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported.

Subscriber hardware assurance signing keys shall not be transferred from the module in which they are generated.

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 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. When pass-phrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For IceCAP-cardAuth Certificates and CIV cardAuth Certificates issued at the Basic Hardware-256 assurance level, user activation of the Private Key is not required.

Activation of private keys stored on an STP shall require multi-factor authentication.

For device and content signing Certificates, the device or CMS 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. 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 Role-Based Code Signing Keys (for signature of Aircraft software/parts)

For Role-Based Code Signing Certificates where the Keys are used to sign Aircraft software/parts and LSAP Code Signing Certificates, the Role sponsor, or the Role Sponsor's employer, shall keep a log stating to whom such role Certificates were issued. This log must be kept for a minimum of thirty (30) years, or as further required by Industry Regulation. 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 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 Ice-CAP-cardAuth, id-basic-device-software-256, id-basic-device-hardware-256, id-medium-device-software-256 and id-medium-device-hardware-256, private keys may be activated without entry of activation data.

For all other policies governed by this CP, 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.

Subscriber activation data presented to an STP in order to access Subscriber keys shall be changed whenever the private key is changed, at a minimum.

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.

Subscriber activation data presented to an STP in order to access Subscriber keys shall be protected from disclosure to unauthorized parties, from eavesdropping, and from replay.

6.4.3 Other aspects of activation data

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

For IceCAP-hardware, the activation data may be reset, upon a successful biometric 1:1 match of the applicant by an RA or a Trusted Agent against the biometrics collected during the identity proofing process (see Section 3.2.3).

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, STP, Administration Workstations, and RA shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Access control restrictions to CA services based on authenticated identity
- 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. This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical controls.

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, CSA, CMS, STP and RA systems shall be configured with the minimum number of required accounts and network services, and no remote login functionality.

Only physical hardware systems shall be used.

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

6.5.2 Computer security rating

The Carillon PKI does not make use of security rating requirements beyond the ones associated with assurance levels.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

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

- 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, CMS, CSA, STP, 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.
- Where open-source software has been utilized, there shall be a demonstration that security requirements were achieved through software verification and validation and structured development/lifecycle management.

6.6.2 Security management controls

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

There shall be a mechanism to periodically verify the integrity of the software and to detect unauthorised modification to the CA, CSA, CMS, and STP 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, CSA, CMS, and STP 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 organization's mission shall be loaded on the RA workstation, and all such software shall be obtained from sources authorized by local policy.

6.6.3 Life cycle security controls

The Carillon PKI does not have any additional life cycle security control requirements.

6.7 Network Security Controls

The Carillon Root CAs and their internal PKI Repositories shall be offline.

Carillon Sub CAs, CSAs, CMSes, STPs, 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, CSA, and STP, 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, CSA, and STP 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, CSA, and/or STP) shall be initiated from the bastion host. The bastion host is considered part of the CA, CMS, CSA, and/or STP 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, CMS, and STP components shall be regularly synchronised 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
- Audit Log Timestamp

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

Section 10 contains the Certificate profiles.

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

CA Certificates shall not include critical private extensions.

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

Carillon Sub 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.

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} i.e. {1.2.840.113549.1.1.11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12} i.e. {1.2.840.113549.1.1.12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13} i.e. {1.2.840.113549.1.1.13}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)} i.e. {1.2.840.10045.4.3.2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha384(3)} i.e. {1.2.840.10045.4.3.3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha512(4)} i.e. {1.2.840.10045.4.3.4}

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}

Where the Certificate contains an elliptic curve public key, the parameters must be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 }

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 RFC5280. 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.

Subject Name Form (Other Subscribers)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, 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, 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-recognized registry and verifiable by the CA (e.g.: aircraft registration / tail number).

Aircraft Equipment Identification shall be an identifier registered in an aerospace industry-recognized 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.

In the case where a Carillon CA certifies another CA within the Carillon PKI, the certifying

Carillon CA shall impose restrictions on the namespace authorised in the subordinate Carillon CA, which are at least as restrictive as its own name constraints.[17]

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

7.1.6 Certificate Policy object identifier

With the exception of self-signed Root CA Certificates, all CA and Subscriber Certificates shall contain at least one Certificate Policy OID listed in section 1.2 of this document.

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

Carillon CAs shall not assert other PKI domains' policy OIDs in the Certificates they issue, with the exception of the *subjectDomain* field in the policy mappings extension of the Cross-Certificates issued to external PKIs.

For non-CA Certificates, the Certificate asserting a policy OID shall also assert all lower assurance policy OIDs, within the restrictions outlined below.

The following restrictions apply to the aforementioned requirements:

- A software Certificate shall not assert a hardware policy OID;
- A "CBP" Certificate shall not assert a non- "CBP" policy OID;
- Role-Based Code Signing Certificates and LSAP Code Signing Certificates used for the signature of Aircraft software/parts shall assert only the medium-hardware-256 or medium-aero-hardware-256 OID(s);
- Role Encryption Certificates used for secret protection shall assert only the id-medium-hardware-256 or medium-aero-hardware-256 OID(s);
- Device Encryption Certificates used for secret recovery shall only assert the id-medium-device-hardware-256 policy OID;
- OCSP Responder Certificates shall assert all policy OIDs for which the issuing CA is authoritative;
- With the exception of content-signers and OCSP responders, Certificates issued to end-entity devices at a medium assurance policy shall assert one of the following policies: id-medium-device-software-256 or id-medium-device-hardware-256;
- With the exception of Certificates issued to aerospace devices, Certificates issued to end-entity devices at a basic assurance policy shall assert one of the following policies: id-basic-device-software-256 or id-basic-device-hardware-256;

[17] This restriction shall be achieved by contractual obligations imposed on the Subordinate CA, as well as through technical configurations on the Subordinate CA. Contracts shall identify Carillon Information Security Inc. as being the sole and final arbiter of the permitted name-space for the Subordinate CA, as having the right to revoke any Certificates issued outside of the permitted namespace, and as having the right to terminate the contract and the CA for non-compliance with said constraint. Technical configurations shall be implemented on the Subordinate CA such that the name constraints identified by Carillon Information Security Inc. are enforced. The latter shall be verified through the use of monitoring software.

- IceCAP-hardware shall only be asserted for Certificates issued to human Subscriber Certificates;
- If IceCAP-cardAuth is asserted, no others shall be asserted;
- If IceCAP-contentSigning is asserted, no others shall be asserted; and
- Under no circumstances can Certificates asserting an IceCAP policy OID (iceCAP-hardware, IceCAP-cardAuth and iceCAP-contentSigning) be used in the context of an STP.

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

ASSURANCE LEVEL[18]	OIDS ASSERTED
basic-device-software-256	id-basicDeviceSoftware-256
basic-hardware-256	id-basicHardware-256 id-basicSoftware-256
basic-device-hardware-256	id-basicDeviceHardware-256 id-basicDeviceSoftware-256
medium-softwareCBP-256	id-mediumSoftwareCBP-256
medium-aero-software-256	id-mediumAeroSoftware-256 id-basicSoftware-256
medium-software-256	id-mediumSoftware-256 id-mediumAeroSoftware-256 id-mediumSoftwareCBP-256 id-basicSoftware-256
medium-device-software-256	id-mediumDeviceSoftware-256 id-basicDeviceSoftware-256
medium-hardwareCBP-256	id-mediumHardwareCBP-256 id-mediumSoftwareCBP-256
medium-aero-hardware-256	id-mediumAeroHardware-256 id-mediumAeroSoftware-256 id-basicHardware-256 id-basicSoftware-256
medium-hardware-256	id-mediumHardware-256

[18] As described in section 1.3.6, CIV Card Authentication and CIV Content Signing are not Assurance Levels.

	id-mediumAeroHardware-256 id-mediumHardwareCBP-256 id-mediumSoftware-256 id-mediumAeroSoftware-256 id-mediumSoftwareCBP-256 id-basicHardware-256 id-basicSoftware-256
medium-device-hardware-256	id-mediumDeviceHardware-256 id-mediumDeviceSoftware-256 id-basicDeviceHardware-256 id-basicDeviceSoftware-256
IceCAP-hardware	id-IceCAPHardware id-mediumHardware-256 id-mediumAeroHardware-256 id-mediumHardwareCBP-256 id-mediumSoftware-256 id-mediumAeroSoftware-256 id-mediumSoftwareCBP-256 id-basicHardware-256 id-basicSoftware-256
IceCAP-cardAuth	id-IceCAPCardAuth
IceCAP-contentSigning	id-IceCAPContentSigning

OCSP Responder Certificates shall assert all the policy OIDs of the Certificates for which the corresponding OCSP Responder provides a revocation status.

7.1.7 Usage of Policy Constraints extension

When present, the policy constraints extension shall be marked critical.

The Carillon 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

The Certificate Policy extension shall not be marked critical.

7.1.10 Inhibit Any Policy extension

If present, this extension shall not be marked critical. SkipCerts shall be set to "0".

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.

All OCSP Responders shall accept and return SHA-1 hashes in the certID and responderID fields. OCSP responses shall not contain a hash algorithm in the certID that differs from the certID in the request.

7.3.1 Version number(s)

The version number for requests and responses shall be v1.

7.3.2 OCSP extensions

Critical extensions shall not be used in OCSP requests or responses.

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.

CAs shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 Frequency or circumstances of assessment

The CAs, CSAs, CMSs, and RAs shall be subject to a periodic compliance audit, which is not less frequent than annually.

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 Carillon PMA has the right to require unscheduled compliance audits of all entities in the Carillon PKI. The Carillon PMA shall state the reason for any unscheduled compliance audit. This compliance audit allows the Carillon PMA to authorise or not (regarding the audit results) the Carillon 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 Carillon Information Security Inc. and its affiliated companies, as well as sub-contractors operating the Carillon PKI. The Carillon PMA shall determine whether a compliance auditor meets this requirement.

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 CPSs, 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 Carillon 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 Carillon PMA of the discrepancy;
- The Carillon PMA shall notify any affected cross-certified external PKI domains' PMAs promptly and provide a remediation plan; 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

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

9.1.2 Certificate access fees

The management of Carillon Information Security Inc. shall decide on any fees related to the Carillon PKI services.

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

9.1.3 Revocation or status information access fees

The management of Carillon Information Security Inc. shall decide on any fees related to the Carillon 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 Carillon Information Security Inc. shall decide on any fees related to the Carillon PKI services.

9.1.5 Refund policy

Carillon Information Security Inc. offers no refunds on issued Certificates.

9.2 Financial responsibility

9.2.1 Insurance coverage

Carillon Information Security Inc. shall maintain reasonable levels of insurance coverage to maintain operations and fulfill obligations as required by applicable laws.

9.2.2 Other assets

Carillon Information Security Inc. 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.

The treatment of confidential business information provided by external PKIs in the context of submitting an application for cross certification will be in accordance with the terms of the agreements entered into between the applicable entity and Carillon Information Security Inc.

9.4 Privacy of personal information

For the purposes of the PKI related services, the Carillon PKI collects, stores, processes and discloses personally identifiable information in accordance with applicable laws and regulations, specifically PIPEDA and the Carillon PKI Privacy Policy which is published at:

https://www.carillon.ca/en/privacy.php

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 Carillon CA shall also protect Personally Identifying Information collected to support cross-certification 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 Carillon 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 Carillon PKI Operational Authority shall not violate intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

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

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

9.5.2 Property Rights in this CP and related CPSs

Carillon asserts that it owns and/or has licensed the Intellectual Property Rights to this CP and related CPS. Furthermore, Carillon reserves all Intellectual Property Rights in this CP and related CPSs 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, Carillon Root CAs' root Public Keys and the root Certificates containing them, including all PCA Public Keys and self-signed Certificates, are the property of Carillon.

9.6 Representations and warranties

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

Additional representations and warranties of Carillon 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 Carillon Root CAs

The Carillon 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 Carillon Subordinate or Cross-Certified CAs

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 and legal purposes, consistent with this and any other applicable CP or CPS.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in this policy represents and warrants that it complies with the stipulations of this policy, and complies with the relevant approved CPS. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber representations and warranties

A Carillon 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 or immediately following Certificate issuance. 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 Carillon 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 Carillon 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 1.3.5.3) shall assume the obligations of Subscribers for the Certificates associated with their components.

9.6.4 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.

9.6.5 Representations and warranties of other participants

The Carillon 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 a Carillon PKI CA Certificate shall conform to the stipulations of this document including operating under a CPS that has been approved by the Carillon 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 authorize the affiliation of Subscribers with that Organisation and shall inform the CA of any severance of affiliation with any current Subscriber.

9.6.5.1 STP Obligations

An STP that securely stores and uses credentials when requested by the Subscribers represents and warrants that it shall conform to the stipulations of this CP, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of this CP and the approved CPS;
- Ensuring that Subscriber private keys are protected from disclosure, modification and destruction at all times; and
- Subscriber private keys are used only when the Subscriber appropriately authenticates to the TSP and requests the use of their key.

An STP that is found to have operated in a manner inconsistent with these obligations shall be subject to action as described in Section 8.5.

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 CARILLON AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY CARILLON AND THE CARILLON PKI ARE PROVIDED "AS IS", AND CARILLON, 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 CARILLON CERTIFICATES, ANY SERVICES PROVIDED BY CARILLON, 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 Carillon to other PKI domains' CAs to which Carillon 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 CARILLON CA ARE DISCLAIMED, AS PERMITTED BY LAW.

FOR ALL OTHER CERTIFICATES OF OTHER ASSURANCE LEVELS, THE TOTAL, AGGREGATE LIABILITY OF EACH CARILLON CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE CARILLON CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND

THE TOTAL LIABILITY OF CARILLON SHALL NOT EXCEED A MAXIMUM OF ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT.

9.9 Indemnities

9.9.1 Indemnification by Customer CAs

To the extent permitted by applicable law, other PKI domains CAs issued Certificates by Carillon agree to indemnify and hold Carillon 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 Carillon 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 Carillon 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 Carillon 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 reliance on a "pass-through" Certificate policy OID, 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 Carillon may include additional indemnity obligations.

9.9.3 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold Carillon 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 Carillon 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 Carillon employees.

9.10 Term and termination

9.10.1 Term

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

Carillon 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 Carillon 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, Carillon PKI OA shall use commercially reasonable methods to communicate with cross certified CAs, taking into account the criticality and subject matter of the communication.

Any planned change to the infrastructure of a Carillon CA that has the potential to affect a cross-certified entity's operational environment shall be communicated to that entity's PMA at least two weeks and one day prior to implementation, and any new artefacts (CA Certificates, CRL DP, AIA URLs, etc.) produced as a result of the change provided to that PMA within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for amendment

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

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

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

Notwithstanding the foregoing, if the Carillon PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of Carillon, the Carillon 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 Carillon 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 thirty (30) days of approval by the Carillon PMA.

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

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

9.12.3 Circumstances under which OID must be changed

Certificate Policy OIDs shall be changed if the Carillon 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 Carillon PMA/OA and Third Parties

Provisions for resolving disputes between the Carillon 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 Carillon 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

Carillon 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.

CARILLON 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 CARILLON.

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.

When using elliptic curve Public Keys, compression of elliptic curve points shall not 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 Carillon 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. The caIssuers field of the AIA extension shall be a pointer to a DER encoded PKCS#7 Certificates only bundle with the extension .p7c. The CRL DP shall be a pointer to a DER encoded CRL with the extension .crl. 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.

Octet String is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits.

CAs may issue partitioned CRLs as long as the CRLs are not indirect CRLs, are not partitioned by reason code, and the CRL DP and issuingDistributionPoint do not assert a name relativeToIssuer. If a CRL does not include issuingDistributionPoint, it must be a full and complete CRL covering all Certificates signed by any and all keys associated with the CA.

If Delta CRLs are implemented, the CRL extension id-ce-freshestCRL must not be marked critical.

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 Carillon PCA → CBCA G3 Certificate

FIELD	VALUE
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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 – G3, ou=Certification Authorities, o=CertiPath, c=US
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
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
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
Subject Information Access	c=no; id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA Certificates issued by the Subject CA. If the Certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points	c = no;

FIELD	VALUE
Inhibit anyPolicy	c=no; skipCerts = 0

10.1.2 Carillon Self-Signed Roots (Trust Anchors)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; keyCertSign, cRLSign, digitalSignature, nonRepudiation
Basic Constraints	c=yes; cA=True; path length constraint absent

10.1.3 Carillon Subordinate CAs

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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 (optional), nonRepudiation (optional)
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints[19]	c=yes; cA=True; pathLength = 0;
Name Constraints	c=no[20]; 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
Subject Information Access	c=no; id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA Certificates issued by the Subject CA. If the Certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.

[19] In general, Basic Constraints path length constraint is set to zero for an issuing CA.

[20] While making this extension critical would be preferable, some widely-distributed certificate validation implementations do not properly process it, causing interoperability issues.

Field	Value
CRL Distribution Points	c = no;

10.1.4 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	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 120 days, 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	Refer to section 7.1.3
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; nonRepudiation (required), digitalSignature (required)
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: HTTP URL for the OCSP Responder (preferred); and/or DNS: Fully qualified domain name of 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

Field	Value
	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

10.1.5 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	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	According to the table in section 5.6, 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	Refer to section 7.1.3
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; nonRepudiation, 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; HTTP URL for the SCVP Server
CRL Distribution Points	c=no

10.1.6 TSA Certificate issued by the Root CA

The following table contains the TSA Certificate profile assuming that the Root CA issues

the TSA Certificate.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	critical=no; <SKI of issuing CA's Signing 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, nonRepudiation
Extended Key Usage	c=yes; 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
CRL Distribution Points	c=no

10.1.7 TSA Certificate issued by the Sub CA

The following table contains the TSA Certificate profile assuming that the Sub CA issues the TSA Certificate.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP

Field	Value
Validity Period	No longer than issuing Sub CA (up to 10 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	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	critical=no; <SKI of issuing CA's Signing 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, nonRepudiation
Extended Key Usage	c=yes; 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
CRL Distribution Points	c=no

10.2 End-Entity Certificates

This section describes the values that populate each field of the Certificates issued by the Carillon PKI CAs.

10.2.1 Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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

Field	**Value**
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
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 for IceCAP-hardware, otherwise 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	Refer to section 7.1.3
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	Refer to section 7.1.3
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), nonRepudiation (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; 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

10.2.3 Subscriber Encryption Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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 if using RSA) or keyAgreement (required if using ecdh), dataEncipherment (optional if using RSA)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[21]	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

[21] Only software OID asserted to support key recovery to software tokens

10.2.4 Code Signing or Role-Based Code Signing Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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), nonRepudiation (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

10.2.5 LSAP Code Signing Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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), nonRepudiation (always present)
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

Field	Value
Applicability[22]	Optional; c=yes; one or multiple OID values representing commercial contexts

10.2.6 Device or Server Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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, only allowed when using RSA) or keyAgreement (optional, only allowed when using ecdsa)
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, 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;

[22] Applicability: Carillon-specific extension (id-ce-applicability {1.3.6.1.4.1.25054.3.6.1}) containing an OID value representing the commercial context in which this certificate should be evaluated.

Field	Value
	id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.7 Device or Server Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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), nonRepudiation (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, 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

Field	Value
CRL Distribution Points	c = no

10.2.8 Device or Server Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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 if using RSA) or keyAgreement (required if using ecdh), dataEncipherment (optional if using RSA)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[23]	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name | RFC822 email address
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

[23] Only software OID asserted to support key recovery to software tokens

Field	Value
CRL Distribution Points	c = no

10.2.9 Device License Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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), nonRepudiation (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, 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

10.2.10 Aircraft or Aircraft Operations Equipment Identity Certificate[24]

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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, only allowed when using RSA) or keyAgreement (optional, only allowed when using ecdsa)
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; Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) | UserPrincipalName (optional)

[24] The term "Aircraft Operations Equipment" applies to On-Aircraft equipment, Ground Support equipment, and Ground Terminals that communicate with the Aircraft.

Field	Value
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

10.2.11 Aircraft or Aircraft Operations Equipment Signature

Certificate[25]

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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), nonRepudiation (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; Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) (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

10.2.12 Aircraft or Aircraft Operations Equipment Encryption

[25] The term "Aircraft Operations Equipment" applies to On-Aircraft equipment, Ground Support equipment, and Ground Terminals that communicate with the Aircraft.

Certificate[26]

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	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	Refer to section 7.1.3
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 if using RSA) or keyAgreement (required if using ecdh), dataEncipherment (optional if using RSA)
Extended key usage	c=no; as per section 10.7
Certificate Policies[27]	c=no; As per section 7.1.6
Subject Alternative Name	c=no; Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) (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
CRL Distribution Points	c = no

[26] The term "Aircraft Operations Equipment" applies to On-Aircraft equipment, Ground Support equipment, and Ground Terminals that communicate with the Aircraft.

[27] Only software OID asserted to support key recovery to software tokens

10.2.13 Role Identity Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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)
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 OCSP Responder

10.2.14 Role Signature Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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), nonRepudiation (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 OCSP Responder

10.2.15 Role Encryption Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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 if using RSA) or keyAgreement (required if using ecdh)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies[28]	c=no; As per section 7.1.6
Subject Alternative Name	c = no; 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

[28] Only software OID asserted to support key recovery to software tokens

10.2.16 IceCAP Card Authentication Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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; id-IceCAPCardAuth 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

10.2.17 IceCAP Content Signer Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	9 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	Refer to section 7.1.3
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; id-IceCAPContentSigning 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

10.2.18 CIV Card Authentication Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
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	Refer to section 7.1.3
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

10.2.19 CIV Content Signer Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	9 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	Refer to section 7.1.3
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

10.3 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	Refer to section 7.1.3
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 Generalized Time)
Issuer's Signature	Refer to section 7.1.3
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 revoked for key compromise or CA compromise

10.3.2 Distribution Point Based Partitioned CRL

Not Supported

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, which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Produced At	Generalized Time
List of Responses	Each response will contain Certificate id; Certificate status[29], thisUpdate, nextUpdate[30],
Responder Signature	Refer to section 7.1.3
Certificates	Applicable OCSP Responder Certificate

[29] If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

[30] The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

Field	**Value**
Response Extension	**Value**
Nonce	(optional) c=no; Value in the nonce field of request (only included if present in the request)[31]
Response Entry Extension	**Value**
None	None

10.6 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests for CAs.

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	Signed using the private key associated with above Subject Public Key
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; keyCertSign, cRLSign, digitalSignature (optional), nonRepudiation (optional)
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC-822, and DNS name forms

[31] An OCSP Responder may operate entirely offline, only pre-generating OCSP Responses that do not include a nonce. If the OCSP Responder is online and available to sign responses, support for inclusion of a nonce is optional.

10.7 Permitted Extended Key Usage Values

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA[32]	None	None	All
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}[33]	None	All Others
Subscriber, Role: Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; Microsoft 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	Any EKU that is not consistent with Key Usage anyExtendedKeyUsage {2.5.29.37.0}
Subscriber, Role Authentication and Signature Certificate (Two Certificate Solution)	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}[34]; id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; Microsoft 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	Any EKU that is not consistent with Key Usage anyExtendedKeyUsage {2.5.29.37.0}

[32] CA Certificate includes: self-signed Root Certificate, Cross-Certificates, intermediate and subordinate CA Certificates, and self-issued key roller Certificates.

[33] smartCardLogon and id-pkinit-KPClientAuth required only if the Private Key is in hardware.

[34] smartCardLogon and id-pkinit-KPClientAuth required only if the Private Key is in hardware.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Subscriber, Role: Encryption[35] with escrow	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} driveEncryption {1.3.6.1.4.1.311.67.1.1} Document Encryption {1.3.6.1.4.1.311.80.1}	Any EKU that is not consistent with Key Usage anyExtendedKeyUsage {2.5.29.37.0}
Role: Encryption without escrow	id-eku-secret-protection {1.3.6.1.4.1.25054.3.8.1}	None	All others
Code Signing, Role-Based 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}[36]	All Others
LSAP Code Signing	id-eku-lsap-code-signing {1.3.6.1.4.1.25054.3.5.1}	None	All Others
License Signing	id-eku-license-signing (1.3.6.1.4.1.25054.3.7.1	None	All Others
Role Based Code Signing for Aircraft Parts	As per Manufacturer's specification or requirement	None	All Others
CIV Card Authentication[37]	id-eku-civ-cardAuth {1.3.6.1.4.1.25054.3.4.1}	None	All Others
CIV Content Signing[38]	id-eku-civ-content-signing {1.3.6.1.4.1.25054.3.4.2}	None	All Others
PIV-I Card Authentication	id-PIV-cardAuth {2.16.840.1.101.3.6.8}	id-pivav-cardAuth {1.3.6.1.4.1.11243 20.1.9}	All Others
PIV-I Content Signing	id-fpki-pivi-content-signing {2.16.840.1.101.3.8.7}	None	All Others

[35] This Certificate is defined as the one that has only the key encipherment or key agreement bit set and optionally data encipherment bit set.

[36] It is recommended that this EKU be included so that Microsoft platforms will not verify signed code using an expired Certificate.

[37] As described in section 1.3.6, CIV Card Authentication Certificates may only assert the basic-hardware-256 Assurance Level.

[38] As described in section 1.3.6, CIV Content Signing Certificates may only assert the basic-hardware-256 Assurance Level.

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
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
Subscriber or Role Authentication, or Device Authentication Certificate used for VPN Client	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
Device Authentication Certificate used for VPN 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}; 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
Subscriber or Role Authentication, or Device Authentication Certificate used for Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	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

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Device Authentication Certificate used for 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
Device Signature used for sending automated emails	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}	None	All Others
Device Signature used for Message Signing (Web Service, Type X, etc.), other than airground communications	id-messageSigning {1.3.6.1.4.1.11243.20.1.1}	None	All Others
Device Encryption used for Message Encryption (Web Service, Type X, etc.), other than airground communications	id-messageEncryption {1.3.6.1.4.1.11243.20.1.2}	None	All Others
Device Encryption used for Database Encryption	id-databaseEncryption {1.3.6.1.4.1.11243.20.1.3}	None	All Others
Device Encryption used for Archive Encryption	id-archiveEncryption {1.3.6.1.4.1.11243.20.1.4}	None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Device Encryption without escrow	id-eku-secret-recovery {1.3.6.1.4.1.25054.3.8.2}	None	All others
Device Signature used for Archive Integrity Protection	id-archiveSigning {1.3.6.1.4.1.11243.20.1.5}	None	All Others
Device Signature used for Assertion Signing (e.g. SAML Assertions by Identity Providers and Attribute Authorities)	id-assertionSigning {1.3.6.1.4.1.11243.20.1.6}	None	All Others
Device Encryption used for Assertion Protection	id-assertionProtection {1.3.6.1.4.1.11243.20.1.12}	None	All Others
Device Signature used for signing air-ground communication messages	id-airGroundCommsSigning {1.3.6.1.4.1.11243.20.1.7}	None	All Others
Device Encryption used for providing confidentiality to airground communication messages[39]	id-airGroundCommsEncryp-tion {1.3.6.1.4.1.11243.20.1.8}	None	All Others

[39] This is for providing confidentiality to other than the transport layer (i.e. NOT SSL/TLS or IPsec communications)

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Bar Coded Boarding Pass Signing	id-BCBPSigning {1.3.6.1.4.1.11243.20.1.11}	None	All Others
Aircraft or Aircraft Equipment Identity	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
Aircraft or Aircraft Equipment Signature	id-airGroundCommsSigning {1.3.6.1.4.1.11243.20.1.7}	None	All Others
Aircraft or Aircraft Equipment Encryption	id-airGroundCommsEncryp-tion {1.3.6.1.4.1.11243.20.1.8}	None	All Others

11 Interoperable Smart Card Definition

IceCAP enables the issuance of smart cards that are technically interoperable with United States Federal Government Personal Identity Verification (PIV) Card readers and applications as well as PIV-Interoperable (PIV-I) card readers and applications. IceCAP fully maps to PIV-I specification as defined by the U.S. Federal Government. This section defines the specific requirements of an IceCAP Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

- Smart card platform shall be from the GSA's FIPS 201 Evaluation Program Approved Product List (APL) and shall use the PIV application identifier (AID). In the event card stock is subsequently found to be unsuitable for PIV-I use, it may be removed from the APL and placed on the Removed Products List. In such cases, the following applies:
  - Card stock that has been placed on the Removed Products List may continue to be issued for no more than one year after GSA-approved replacement card stock is available.
  - Once replacement card stock has been available for one year, PIV-I cards issued using card stock that has been placed on the Removed Products List may continue to be used until the current subscriber Certificates expire, unless otherwise notified.
- Smart card shall contain a Private Key and associated Identity Certificate asserting the IceCAP-hardware Certificate Policy OID.
- Smart card shall contain a Private Key and associated Card Authentication Certificate asserting the IceCAP-cardAuth Certificate Policy OID.
- Smart card may contain a Private Key and associated Digital Signature Certificate asserting the medium-hardware Certificate Policy OID.
- Smart card may contain a Private Key and associated Encryption Certificate asserting the medium-software Certificate Policy OID.
- A digital signature Certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain the Carillon id-IceCAPContentSigning policy OID.
- Smart card shall contain Identity, Signature, Encryption, and IceCAP Card Authentication Certificates that conform to the applicable profiles in Section 10.
- Smart card shall contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder Facial Image printed on the card.
- Smart card and all data objects on it shall be issued in accordance with SP 800-73.
- Biometrics on the smart card shall also comply with Section 4.2.3 of FIPS 201-3 and SP 800-76.
- Cardholder Unique Identifier (CHUID) shall also comply with FIPS 201. The CHUID shall contain 16 byte Global Unique Identifier (GUID).
- The CMS-Signed objects such as fingerprint and photograph shall contain GUID as

entryUUID attribute in place of FASC-N as pivFASC-N attribute.

- Smart cards shall be visually distinct from the US Federal PIV Card. At a minimum, images or logos on an IceCAP Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].
- The smart card physical topography shall include, at a minimum, the following items on the front of the card:
  - Cardholder facial image; and
  - Cardholder full name; and
  - Organizational Affiliation, if it exists; otherwise the issuer of the card; and
  - Card expiration date.
- Smart card shall have an expiration date not to exceed 3 years of issuance.
- Expiration of the IceCAP Content Signing Certificate on the card shall be later than the expiration of the Subscriber Certificates on the card.[40] The Content Signing Certificate shall conform to the Content Signing Certificate profile specified in Section 10.
- The IceCAP Content Signing Certificate and corresponding Private Key shall be managed within a trusted CMS in accordance with the requirements specified in this document.
- At issuance, the RA shall activate and release the smart card to the Subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected during identity-proofing (See Section 3.2.3).

Smart card may support card activation by the CMS to support card personalization and post-issuance card update. To activate the card for personalization or update, the CMS shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP 800-73]. When cards are personalized, card management keys shall be set to be specific to each smart card. That is, each smart card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in [SP 800-78].

On an annual basis, one populated representative PIV-I smart card must be submitted for testing to the FIPS 201 Evaluation Program for each smart card platform and configuration in use by the Carillon PKI.

11.1 Acceptable Identity Source Documents

At least one identity source document shall meet the requirements of Strong evidence as specified in [SP 800-63A] and be one of the following forms of identification:

- U.S. Passport or U.S. Passport Card
- Driver's license or ID card that is compliant with [REAL-ID] requirements
- Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
- Foreign Passport

[40] It is recommended that expiration of the Content Signing Certificate be later than expiration of the card.

- Employment Authorization Document that contains a photograph (Form I-766)
- PIV Card

The second piece of evidence may be from the list above, but it shall not be of the same type as the primary identity source document. The second identity source document may also be one of the following:

- ID card issued by a federal, state, or local government agency or entity, provided that it contains a photograph
- Voter's registration card
- U.S. Coast Guard Merchant Mariner Card
- Certificate of U.S. Citizenship (Form N-560 or N-561)
- Certificate of Naturalization (Form N-550 or N-570)
- U.S. Citizen ID Card (Form I-197)
- Identification Card for Use of Resident Citizen in the United States (Form I-179)
- Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350)
- Reentry Permit (Form I-327)
- Employment authorization document issued by the Department of Homeland Security (DHS)
- Driver's license issued by a Canadian government entity
- Native American tribal document
- U.S. Social Security Card issued by the Social Security Administration
- Original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal
- Another piece of evidence that meets the requirements of Fair evidence specified in [SP 800-63A]