Carillon INFORMATION SECURITY

We Build TRUST

Boeing Airplane Software Signing PKI Certificate Policy

Jason Griffith
PMA Chair

Prepared by: Carillon Information Security
Updated on: August 28, 2023
Version: 1.3
Classification: Public
Status: FINAL

Version Information

Version	Date	Author	Notes
1.0 – RC	October 27, 2021	Carillon Information Security	Release Candidate
1.0	November 5, 2021	Carillon Information Security	Final version – Approved by Boeing Airplane Software Signing PKI Policy Management Authority on November 5th 2021.
1.1	April 4, 2022	Carillon Information Security	CR-01 - Minor adjustments Add content in Section 1.6.2 – Acronyms Throughout the document – Minor typographical and formatting adjustments. CR-02 – Modify the Subject Name Form for End-Entity Certificates Modify content in the following section: 7.1.4 Version 1.1 approved by Boeing Airplane Software Signing PKI Policy Management Authority on April 4th, 2022.
1.2	April 10, 2023	Carillon Information Security	CR-01 - Minor adjustments PMA Co-Chair change - Modify content in the following section: 1.5.2 CR-02 – Add 8.7 Retention of Audit report section – required for SPEC-42 compliance Add content in following section: 8 CR-03 – Modify sections 9.3 and 9.4 for RFC 3647 compliance Modify and add content in the following sections: 9.3, 9.4 CR-04 - Add an OU option in the Name Forms Modify content in the following section: 7.1.4 Version 1.2 approved by Boeing Airplane Software Signing PKI Policy Management Authority on April 10th, 2023.
1.3	August 28, 2023	Carillon Information Security	CR-01 - Minor adjustments PMA Co-Chair change - Modify content in the

			following section: 1.5.2 CR-02: Add a reference to Spec 42 and associated definition and acronyms Modify content in the following sections: 1; 1.6.1; 1.6.2 CR-03: Modify profile for LSAP Signing Certificate (SAN, code-signing EKU) Modify content in the following sections: 10.2.1; 10.7 Version 1.3 approved by Boeing Airplane Software Signing PKI Policy Management Authority on August 28, 2023.

Table of Contents

1 Introduction

The Boeing Airplane Software Signing PKI is a PKI that accommodates programs that carry out or support the mission of The Boeing Company (Boeing) that require authentication, confidentiality, non-repudiation, and access control.

This Certificate Policy defines one policy to support the Boeing Airplane Software Signing PKI.

This policy represents the following Assurance Level for Public Key Certificates:

- id-mediumDeviceHardware-sw-parts-signing-256

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.

This policy covers the Boeing Airplane Software Signing PKI Root CA and the certified subordinated Boeing Airplane Software Signing PKI Sub CAs.

Any use of, or reference to this CP outside the purview of the Boeing Airplane Software Signing PKI Policy Management Authority is completely at the using party's risk.

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.

This CP complies with the requirements of the ATA DSWG Reference Certificate Policy in ATA Spec 42 - Aviation Industry Standards for Digital Information Security.

1.1 Overview

1.1.1 Certificate Policy (CP)

Certificates issued by the Boeing Airplane Software Signing PKI 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.

Please note that this Certificate Policy includes features and requirements that are not currently implemented in the PKI, such as:

- Human Subscribers
- Devices Certificates for IT infrastructure (such as routers, firewalls, servers, etc.)
- Encryption Certificates and key escrow
- Role Certificates

- SCVP Servers
- Time-Stamp Authority (TSA)

Those features have been included in the document for easier mapping with other Certificate Policies and for possible future expansion of PKI activities with the approval by the Boeing Company PKI Policy Authority Board and the Boeing Airplane Software Signing PMA.

1.1.2 Relationship between this CP and a Boeing Airplane Software Signing CPS

This CP states what assurance can be placed in a Certificate issued under this policy. The Boeing Airplane Software Signing PKI CPSs state how the Boeing Airplane Software Signing PKI CAs establish that assurance.

1.1.3 Boeing Airplane Software Signing PKI Scope

Figure 1 illustrates the scope of this CP.

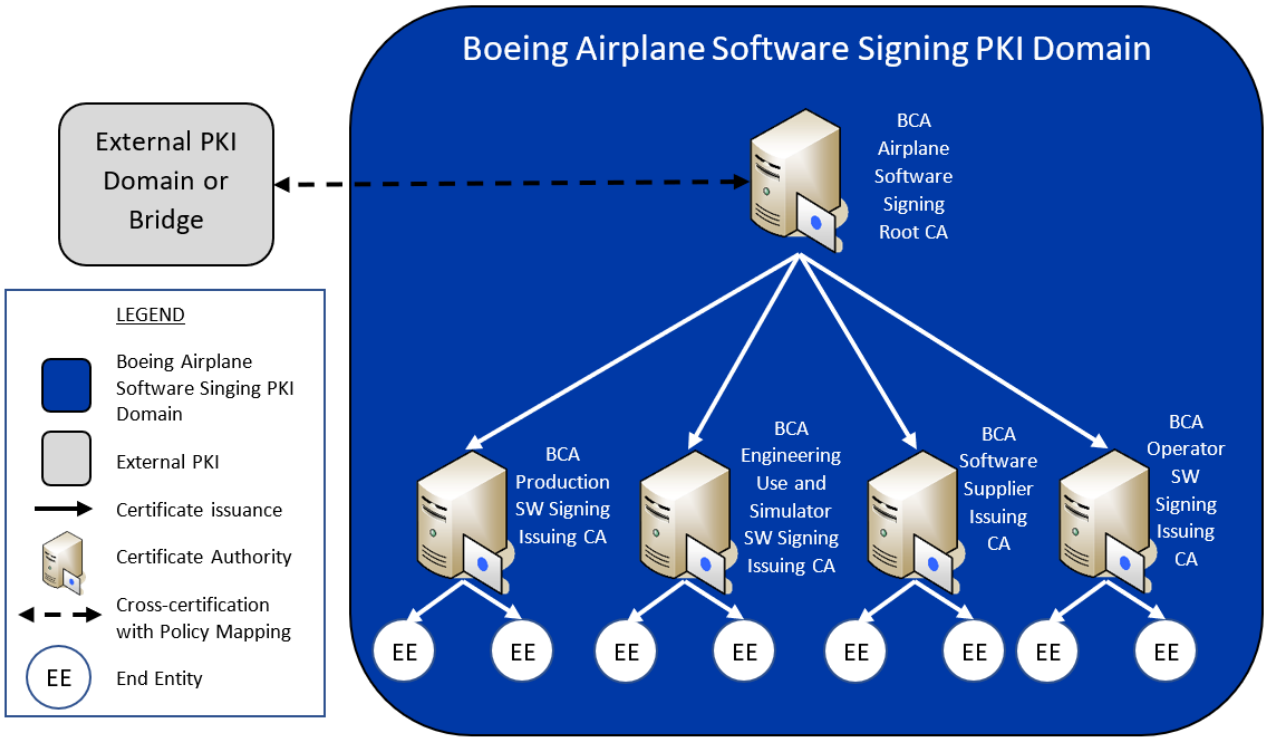

Figure 1 – Scope and Domain of Boeing Airplane Software Signing CAs

This CP imposes requirements on all the Boeing Airplane Software Signing PKI CAs. These include the following:

- the BCA (Boeing Commercial Airplanes) Airplane Software Signing Root Certification Authority
    - BCA Airplane Software Signing Root CA
- all Boeing Airplane Software Signing PKI Certification Authorities subordinated to the BCA Airplane Software Signing Root CA (Boeing Airplane Software Signing Sub CAs):
    - BCA Production SW Signing Issuing CA
    - BCA Engineering Use and Simulator SW Signing Issuing CA
    - BCA Software Supplier Issuing CA
    - BCA Operator SW Signing Issuing CA

The BCA Airplane Software Signing Root CA shall issue CA Certificates only to Boeing Airplane Software Signing Sub CAs approved by the Boeing Airplane Software Signing PKI PMA.

The BCA Airplane Software Signing Root CA may also issue Certificates to individuals who operate the BCA Airplane Software Signing Root CA or devices necessary for the operation of the BCA Airplane Software Signing Root CA.

Boeing Airplane Software Signing 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 Boeing Airplane Software Signing PKI Root CAs and Boeing Airplane Software Signing PKI Sub CAs exist to facilitate trusted communications within the Boeing Domain and with Boeing partners, suppliers, customers, and regulatory authorities.

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 Boeing Airplane Software Signing PKI Root CAs and Boeing Airplane Software Signing PKI Sub CAs.

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

Requirements that apply to a specific CA type will be denoted by specifying the CA type, e.g., Root CA, Sub 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 Boeing Airplane Software Signing PKI Certificate Policy (CP).

Each Assurance Level is uniquely represented by an “object identifier” (OID), which is asserted in each Certificate issued by the Boeing Airplane Software Signing PKI Sub CAs that complies with the policy stipulations under this CP.

The OIDs are registered under the Boeing arc as follows:

Certificate Name	OID
id-boeing	::= {1.3.6.1.4.1.73}
id-security	::= {id-boeing 15}
id-pki	::= {id-security 3}
boeing-certificate-policies	::= {id-pki 1}
Boeing-airplanesoftwaresigning-policies	::= {boeing-certificate policies 42}
id-mediumDeviceHardware-sw-parts-signing-256	::= {Boeing-airplanesoftwaresigning-policies 1}

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

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 Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI Authorities

1.3.1.1 Boeing Airplane Software Signing PKI Policy Management Authority (Boeing Airplane Software Signing PKI PMA)

The Boeing Airplane Software Signing PKI PMA is responsible for:

- Commissioning, drafting and approving the Boeing Airplane Software Signing PKI CP (this document);
- Commissioning compliance analysis, acting on recommendations resulting from analysis, and approving the Boeing Airplane Software Signing PKI CPSs; and
- Ensuring continued conformance of the Boeing Airplane Software Signing PKI CPSs with applicable requirements as a condition for continued securing of the Assurance Levels as stipulated in this CP.

A complete description of Boeing Airplane Software Signing PKI PMA roles and responsibilities is provided in the Boeing Airplane Software Signing PKI Policy Management Authority Charter [PMA Charter and bylaws].

1.3.1.2 Boeing Airplane Software Signing PKI Operational Authority (OA)

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

1.3.1.3 Boeing Airplane Software Signing PKI Operational Authority Administrator (OAA)

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

The Administrator is selected by and reports to the Boeing Airplane Software Signing PKI PMA.

The Administrator approves the assignment of Certificates to the other trusted roles operating the Boeing Airplane Software Signing PKI CAs.

1.3.1.4 BCA Airplane Software Signing Root CA

A Boeing Airplane Software Signing PKI Root CA is a trust anchor for Relying Parties trying to establish the validity of a Certificate issued by a Boeing Airplane Software Signing PKI Sub CA, whose chain of trust can be traced back to that specific Root CA.

A Boeing Airplane Software Signing PKI Root CA issues and revokes Certificates to Boeing Airplane Software Signing Sub CAs upon authorization by the Boeing Airplane Software Signing PKI PMA. As operated by the Operational Authority, a Boeing Airplane Software Signing PKI 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.

1.3.1.5 Boeing Airplane Software Signing PKI Subordinate CAs

The Boeing Airplane Software Signing PKI Sub CAs are all of the Boeing Airplane Software

Signing PKI Signing CAs subordinate to a Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI 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.

1.3.1.6 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.

A Boeing Airplane Software Signing PKI Root CA must not provide Certificate status via OCSP.

1.3.1.7 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.

1.3.1.8 Card Management System (CMS)

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

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 Boeing Airplane Software Signing PKI Operational Authority acts as the RA for the Boeing Airplane Software Signing PKI Root CA. It performs its function in accordance with the relevant Boeing Airplane Software Signing PKI CPS approved by the Boeing Airplane Software Signing PKI 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.

Boeing Airplane Software Signing PKI Root CA Subscribers shall include only timestamping authorities, when approved by the Boeing Airplane Software Signing PKI PMA.

Boeing Airplane Software Signing PKI Sub CA Subscribers may include Boeing employees, Boeing subcontractors' personnel, Boeing suppliers, Boeing partners, Boeing customers, hardware devices (i.e., devices used for LSAP Signing, OCSP responders), and others having to operate and/or do business or act in any lawful capacity within the global air transport or aerospace community.

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 Boeing Airplane Software Signing PKI CAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors. The Boeing Airplane Software Signing PKI 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 for Certificates. The Device Sponsor works with the RAs to register components 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 and that was issued by the Boeing Airplane Software Signing PKI or by another PKI approved by the Boeing Airplane Software Signing PKI PMA.

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 Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI 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 the 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
id-mediumDeviceHardware-sw-parts-signing-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.

In addition to the above:

LSAP Signing Certificates issued under this CP, in which the function 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.

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 Boeing Airplane Software Signing PKI PMA or the Boeing Airplane Software Signing PKI 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

1.4.1 Appropriate Certificate uses

The Boeing Airplane Software Signing PKI CAs will issue digital Certificates to Subscribers for signing software that is to be loaded onto an aircraft system.

This list of use cases for digital Certificates issued by Boeing Airplane Software Signing PKI CAs may be extended with approval from the Boeing Airplane Software Signing PKI PMA.

1.4.2 Prohibited Certificate uses

Prohibited applications include the following:

- any export, import, use or activity that contravenes any local or international laws or regulations;
- any usage of Certificates in conjunction with illegal activities;
- any usage of Certificates for personal use or purposes not related to the community's business;
- any use of a Certificate after it has been suspended or revoked; and
- any use inconsistent with the key usage, extended key usage, or basic constraints specified Certificate profiles/templates (section 10 of this CP) or as approved and documented by the Boeing Airplane Software Signing PMA.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The Boeing Airplane Software Signing PKI PMA is responsible for all aspects of this CP.

1.5.2 Contact persons

Questions regarding this CP shall be directed to the Boeing Airplane Software Signing PKI PMA represented by:

Brien Hansen – Co-Chair of the Boeing Airplane Software Signing PKI PMA

Mail Code: 8J-206
PO Box 3707
Seattle, WA 98124-2207

Jason Griffith – Co-Chair of the Boeing Airplane Software Signing PKI PMA

3003 West Casino Rd
Everett, WA 98204
Mail box: 084-55

1.5.3 Person determining CPS suitability for the policy

The Boeing Airplane Software Signing PKI PMA shall commission an analysis to determine whether the Boeing Airplane Software Signing PKI CPSs conform to the Boeing Airplane Software Signing PKI CP.

When such a compliance analysis shall be performed:

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

1.5.4 CPS approval procedures

The CPS shall be more detailed than the corresponding Certificate Policy described in this document. The Boeing Airplane Software Signing 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 [Boeing Airplane Software Signing PKI PMA Charter and bylaws].

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

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

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

Affiliated Organization - Organizations that authorize affiliation with Subscribers for the issuance of 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 Authorized Subscriber to be named in a Certificate and verifying that such Authorized 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 Authorized 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 authorized Subscriber; producing a digital Certificate containing that and other pertinent information; and digitally signing the Certificate.

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

Within this document, the term CP, when used without qualifier, refers to the Boeing Airplane Software Signing PKI 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.

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 The Boeing Company.

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 authorization.

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 some enrollment processes.

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 Boeing or a Boeing Business Unit and external PKI Domains legal Representation allowing interoperation between the respective Boeing Airplane Software Signing PKI CAs and an external PKI domains CA.

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 organization.

Operational Authority (OA) - An agent of the Boeing Airplane Software Signing 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 Authority Administrator (OAA) - The Operational Authority Administrator is the individual within the Operational Authority who has principal responsibility for overseeing the proper operation of the Boeing Airplane Software Signing PKI infrastructure components.

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.

Organization - 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 organizational 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.

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 Boeing Airplane Software Signing 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 Boeing 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.

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

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

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

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

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

Spec 42 - The Spec 42*: Aviation Industry Standards for Digital Information Security* guidance document, prepared and published by the A4A trade association and lobbying group. It provides recommendations on standardized methods for the integration of digital identity in the operation of modern aircraft in civil aviation.

Sponsoring Organization - An organization with which an Authorized 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 authorized 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

A4A	Airlines For America, formerly known as ATA
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One Encoder / Decoder
ATA	Air Transport Association, renamed Airlines For America (A4A)
BCA	Boeing Commercial Airplanes
C	Country
CA	Certification Authority
CASA	Certification Authority System Administrator
CBP	Commercial Best Practices
CHUID	Cardholder Unique Identifier
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DSWG	Digital Security Working Group
DN	Distinguished Name
DNS	Domain Name Service

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
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organization 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	Organization
OA	Operational Authority
OAA	Operational Authority Administrator
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PACS	Physical Access Control System
PCA	Principal Certification Authority
PDS	PKI Disclosure Statement
PII	Personally Identifiable Information

PIN	Personal Identification Number
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
SOP	Standard Operating Procedure
SSCD	Secure Signature-Creation Devices
SSL	Secure Sockets Layer
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 Boeing Airplane Software Signing PKI operates Repositories containing all information necessary to provide lookup and validation services for issued Certificates.

The mechanisms used by the Boeing Airplane Software Signing 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 Boeing Airplane Software Signing PKI CP shall be published electronically on the Boeing Airplane Software Signing PKI web site.

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

All CRLs, ARLs, and CA Certificates issued by Boeing Airplane Software Signing PKI CAs shall be published to the Boeing Airplane Software Signing PKI respective and applicable Repositories as set forth in the applicable CPSs. Furthermore, all of the above shall be accessible via HTTP.

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 Boeing Airplane Software Signing PKI 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 delegated OCSP service, as described in Section 2.6 of RFC 6960.

2.2.2 Interoperability

The Boeing Airplane Software Signing PKI shall not publish CA Certificates and CRLs in an LDAP directory.

2.2.3 Privacy of information

A Boeing Airplane Software Signing PKI CA or RA shall respect the privacy of Subscribers and Subscribers' Employers.

2.3 Time or frequency of publication

Boeing Airplane Software Signing 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. Certificates and Certificate status information shall be published as specified in section 4 of this CP.

2.4 Access controls on repositories

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

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

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

This CP shall be publicly available through the Internet.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

For Certificates issued to human Subscribers, the subject DN shall either contain the 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).

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][1]Surname.

- For devices:

  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.);

A Boeing Airplane Software Signing PKI Root CA shall impose restrictions on the namespace authorized to that Boeing Airplane Software Signing PKI Sub CA which are at least as restrictive as its own name constraints.

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

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

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

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

3.1.3 Anonymity or pseudonymity of Subscribers

CA Certificates shall not contain anonymous or pseudonymous identities.

Certificates issued by Boeing Airplane Software Signing PKI CAs shall not contain anonymous or pseudonymous identities, only names as defined in section 7 and as stipulated in section 3.1.2.

3.1.4 Rules for interpreting various name forms

Rules for interpreting name forms shall be contained in the applicable Certificate profile.

The authority responsible for Boeing Airplane Software Signing PKI namespace control is the Boeing Airplane Software Signing PKI PMA.

3.1.5 Uniqueness of names

Name uniqueness across the Boeing Airplane Software Signing PKI namespace domains shall be enforced. The Boeing Airplane Software Signing PKI CAs and RAs shall enforce name uniqueness within their authorized 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 names).

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

In the case of a Device that is not capable of generating its own keys, this may only be

possible from a separate computer before the key is transferred onto the Device. Subsequent to proof of possession, the private key shall be distributed to the Device in a manner consistent with section 6.2.

3.2.2 Authentication of organization identity

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

- Full organization legal name;
- Address of its head office;
- Documentation of the existence of the organization (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 authorized representative officially requesting said Certificate.

In all cases, the existence of an affiliated organization 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 authorization to act in the name of the organization. Moreover, requests for end user Certificates other than unaffiliated Subscribers shall include the name of the organization and shall be verified with the identified affiliated organization.

3.2.3 Authentication of individual identity

The Boeing Airplane Software Signing PKI 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.

3.2.3.1 Authentication of Individuals

CAs and RAs are responsible for ensuring that they are in compliance with all applicable laws when collecting personally identifiable information. If a jurisdiction prohibits the collection, distribution or storage of any of the information specified in this section, an alternate, equivalent proofing mechanism may be used that assures the identity of the applicant to an equivalent level, subject to approval of the Boeing Airplane Software Signing PKI PMA.

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification; and

- A signed declaration by that person that he or she verified the identity of the applicant as required by this CP which may be met by establishing how the applicant is known to the verifier as required by this CP , using the format set forth at [28 U.S.C. 1746 -- Unsworn Declarations Under Penalty Of Perjury] or comparable procedure under local law; The signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued, and that was issued by the Boeing Airplane Software Signing PKI or by another PKI approved by the Boeing Airplane Software Signing PKI PMA;

For Basic Assurance Level Certificates, 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 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.

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;
- unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant;
- the date and time of the verification; and
- a declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note). This shall be performed in the

presence of the person performing the identity authentication.

PRACTICE NOTE:

In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature Certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and Certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity, then the Certificate must be revoked.

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

- present one (1) valid National Government-issued photo ID, one valid U.S. State REAL ID Act-compliant picture ID[2], 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.

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 Certificates asserting the Medium Assurance levels, identity shall be established by in-person or remote 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.

When performing in-person proofing 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 Component Identities

Some computing and communications components 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 providing the following registration information:

- Equipment identification (e.g. IP address, hostname, aircraft registration number, aircraft/equipment part number) or service name (e.g., DNS name or function name)

[2] 3REAL ID Act-compliant IDs are identified by the presence of the U.S. Department of Homeland Security REAL ID star.

sufficient to uniquely identify the Subject;

- Equipment Public Keys;
- Equipment authorizations 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, and that were issued by the Boeing Airplane Software Signing PKI or by another PKI approved by the Boeing Airplane Software Signing PKI PMA); 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 organization:

1. The applicant shall personally appear before a verifier (usually a Trusted Agent);
2. The applicant and the verifier shall have an established working relationship with the sponsoring organization. The relationship shall be sufficient to enable the verifier to, with a high degree of certainty, verify that the applicant is the same person that was identity proofed. An example to meet this requirement is when the applicant and Trusted Agents are employed by the same company and the company badge forms the basis for the applicant authentication;
3. The applicant shall present a valid sponsoring organization-issued photo ID. This photo ID shall have been issued on the basis of in-person identity proofing using one valid National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver’s License);
4. The verifier shall record the following:
5. His/her own identity;
6. Unique identifying number from the Identifier (ID) of the verifier;
7. Unique identifying number from the applicant’s sponsoring organization-issued photo ID;
8. Date and time of the identity verification; and

9. Date and time of sponsoring organization-issued photo ID, if applicable.
10. The verifier shall sign a declaration that he or she verified the identity of the applicant as required by the applicable Certificate policy which may be met by establishing how the applicant is known to the verifier as required by this Certificate policy; and
11. The applicant shall sign a declaration of identity using a handwritten signature or appropriate digital signature. This declaration shall be signed in the presence of the verifier.

3.2.3.4 Authentication of Human Subscriber for Role Certificates

Human Subscribers may be issued Role Certificates[3]. 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.

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

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

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

The procedures for issuing Role Certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of 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.

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

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.

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

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

3.2.5 Validation of authority

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

3.2.6 Criteria for interoperation

It is the responsibility of the Boeing Airplane Software Signing PKI PMA to ensure the requirements below are met prior to authorizing any kind of interoperation agreement.

Interoperating CAs shall adhere to the following requirements before being approved by the Boeing Airplane Software Signing PKI PMA for interoperation:

- Have a CP determined by the Boeing Airplane Software Signing PKI 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;
- 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

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

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

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

Assurance level	Further requirements
mediumDeviceHardware-sw-parts-signing-256	The initial identity-proofing process must be carried out at least once every three (3) years

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, unless he/she can be authenticated through the use of a valid public key Certificate of equal or higher assurance, as specified in Section 3.3.1.

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 Certificate being managed. For example, a web site secured using SSL 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 of the Boeing Airplane Software Signing PKI or another PKI approved by the Boeing Airplane Software Signing PKI PMA, 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 Boeing Airplane Software Signing PKI Root CA, an authorized representative of the Subject CA shall submit the application to the Boeing Airplane Software Signing PKI PMA.

4.1.2 Enrolment process and responsibilities

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

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

applicable CPS.

For CA Certificates, the Boeing Airplane Software Signing PKI PMA shall verify all authorizations 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 9.6.3.

4.1.2.1 End-Entity Certificates

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

- establish and record identity of Subscriber (per section 3.2);
- obtain a public/private Key Pair for each Certificate required; and
- establish that the Public Key forms a functioning Key Pair with the Private Key held by the Subscriber (per section 3.2.1).
- provide a point of contact for verification of any roles or authorizations 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 Boeing Airplane Software Signing PKI PMA shall establish its criteria and procedures describing how Sub CAs may apply for and receive a Certificate from a Boeing Airplane Software Signing PKI Root CA.

A Boeing Airplane Software Signing PKI Root CA shall certify Boeing Airplane Software Signing PKI Sub CAs implementing this CP only as authorized by the Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI Sub CA.

The Boeing Airplane Software Signing PKI 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.

The Boeing Airplane Software Signing PKI PMA shall commission a CPS compliance analysis prior to authorising the OA to issue and manage CA Certificates asserting this CP.

Boeing Airplane Software Signing PKI CAs shall only issue Certificates asserting the OIDs

outlined in this CP upon receipt of written authorization from the Boeing Airplane Software Signing PKI PMA, and then may only do so within the constraints imposed by the Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI 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

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

4.2.2 Approval or rejection of Certificate applications

The Boeing Airplane Software Signing PKI CAs, respective RAs, or the Boeing Airplane Software Signing PKI PMA may approve or reject a Certificate application.

For CAs the Boeing Airplane Software Signing PKI 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;
- 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.

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

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 Boeing Airplane Software Signing PKI OA shall inform the Boeing Airplane Software Signing PKI PMA of any Certificate issuance to a CA by a Boeing Airplane Software Signing PKI Root CA. The Boeing Airplane Software Signing PKI PMA shall inform the authorized instance of such applicant CA of the successful Certificate issuance.

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.

For the issuance of CA Certificates to Boeing Airplane Software Signing PKI Sub CAs, the Boeing Airplane Software Signing PKI PMA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate issuance by the CA to other entities

No stipulation.

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

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

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by section 1.4.1 or 1.4.2. CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate;
- that the Certificate is being used in accordance with the keyUsage,

extendedKeyUsage, and certificatePolicies field extensions included in the Certificate; and

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

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 must 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 the same name, key, and other information as the old one, with a new extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. After Certificate renewal, the old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

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

4.6.1 Circumstance for Certificate renewal

A Certificate may be renewed if the Public Key has not reached the end of its validity period, the associated Private Key has not been revoked or compromised, and the Subscriber name

and attributes are unchanged. In addition, the validity period of the Certificate must not exceed the remaining lifetime of the Private Key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2 Who may request renewal

A Device Sponsor may request renewal of an OCSP Certificate.

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.

4.6.4 Notification of new Certificate issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate issuance by the CA to other entities

See Section 4.4.3.

4.7 Certificate Re-Key

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

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

4.7.1 Circumstance for Certificate re-key

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

4.7.2 Who may request certification of a new Public Key

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

A Role Sponsor may request 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 component Certificate they have sponsored.

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 Boeing Airplane Software Signing PKI 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

Updating a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old Certificate. For example, a Boeing Airplane Software Signing PKI 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 further re-keyed, renewed, or updated.

Certificate modification is only supported by this CP for CA Certificates.

4.8.1 Circumstance for Certificate modification

A CA may issue a new Certificate to the Subject when some of the Subject information has changed, 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 Boeing Airplane Software Signing PKI CA 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.

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 Organizations that the Organization 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 authorized 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.

4.9.2 Who can request revocation

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

For Role Signature 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.

For CA Certificates, authorized individuals representing the CA Operational Authority may request revocation of Certificates.

Notwithstanding the above, a Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI 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, authorized 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 Boeing Airplane Software Signing PKI Root CA, the Operational Authority shall seek guidance from the Boeing Airplane Software Signing PKI PMA before revocation of the Certificate except when the Boeing

Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI.

For Certificates issued by a Boeing Airplane Software Signing PKI Sub CA whose operation involves the use of a cryptographic hardware token, a Subscriber ceasing its relationship with the organization that sponsored the Certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be returned to Boeing Airplane Software Signing PKI 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 organization 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.

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

For Boeing Airplane Software Signing PKI Sub CAs, processing time for Subscriber Certificate revocation requests shall be as specified below:

Assurance Level	Processing Time for Revocation Requests
medium-device-hardware-256	Before next CRL is generated unless request is received within 2 hours of CRL generation

4.9.6 Revocation checking requirement for Relying Parties

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

standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL issuance frequency

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

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

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of Certificate status information for 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.

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 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

The Boeing Airplane Software Signing PKI CAs are not required to operate an OCSP Responder covering the Certificates they issue.

The Boeing Airplane Software Signing PKI Repository shall contain and publish a list of all OCSP Responders operated by the Boeing Airplane Software Signing PKI 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 optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

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

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

4.9.10 On-line revocation checking requirements

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

Certificate suspension is not supported by this Certificate Policy.

4.9.14 Who can request suspension

Certificate suspension is not supported by this Certificate Policy.

4.9.15 Procedure for suspension request

Certificate suspension is not supported by this Certificate Policy.

4.9.16 Limits on suspension period

Certificate suspension is not supported by this Certificate Policy.

4.10 Certificate status services

The Boeing Airplane Software Signing PKI is not required to support Server-based Certificate Validation Protocol (SCVP) or Online Certificate Status Protocol (OCSP).

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

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

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.

4.10.3 Optional features

No stipulation.

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 Boeing Airplane Software Signing PKI CAs that escrow the private keys of encryption Certificates at Medium or higher Assurance Levels, a Key Recovery Practise Statement ([KRPS]) shall be developed.

4.12.2 Session key encapsulation and recovery policy and practices

This Certificate Policy does not support the recovery of session keys.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA, CSA, and CMS equipment shall always be protected from unauthorized access. The physical security requirements pertaining to CA, CSA, and CMS equipment are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Provide at least three (3) layers of increasing security such as perimeter, building, and CA room
- Require two (2) person physical access control to both the cryptographic module and computer system
- 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.

A security check of the facility housing the CA, CSA, and CMS equipment 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 unauthorized 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 unauthorized 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 standard data centre procedures. CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic), theft and 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 – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
- Registration Authority – authorized to request or to approve Certificates or Certificate revocations.
- Audit Administrator – authorized to view and maintain audit logs.
- Operator – authorized 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; and
- 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; and
- 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.

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.

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

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. See section 6.7 for authentication to the PKI equipment.

5.2.4 Roles requiring separation of duties

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

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

- Individuals who assume a Registration Authority role may not assume an Administrator role; and
- Individuals who assume an Audit Administrator role shall not assume any other role.
- Under no circumstances shall any of the four roles perform their own compliance auditor function.

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

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

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

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

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

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

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

For RAs and Trusted Agents, 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, and RA roles shall have completed a background investigation as allowed by applicable national law or regulation. The scope of the background check shall include the following areas covering the past five (5) years and should be refreshed every three (3) years:

- Employment;
- Education (Regardless of the date of award, the highest educational degree shall be verified);
- Place of residence (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.

When the background investigation is performed as part of a security clearance, the security clearance must be 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. When a formal security clearance is the basis for the background screening, the background procedure is part of the formal security screening process. The background refresh shall be in accordance with the corresponding security clearance.

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

Training shall be conducted in the following areas:

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

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The Boeing Airplane Software Signing PKI 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, or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of section 5.3).

5.3.8 Documentation supplied to personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of events recorded

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

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

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- A message from any source requesting an action by a CA is an auditable event. The message must include message date and time, source, destination and contents.

The following events shall be audited[4]:

Auditable Event	CA	CSA	RA	CMS
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X
Obtaining a third-party time-stamp	X	X	X	X
IDENTITY-PROOFING				
Successful and unsuccessful attempts to assume a role	X	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X

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

LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	X	X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	X	X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	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
PRIVATE KEY LOAD AND STORAGE				
The loading of Component Private Keys	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
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	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
CERTIFICATE REGISTRATION				
All Certificate requests	X	N/A	X	X
CERTIFICATE REVOCATION				
All Certificate revocation requests	X	N/A	X	X
CERTIFICATE STATUS CHANGE APPROVAL				

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

Receipt of hardware / software	X	X	X	X
Attempts to set passwords	X	X	X	X
Attempts to modify passwords	X	X	X	X
Back up of the internal CA database	X	N/A	N/A	X
Restoration from back up of the internal CA database	X	N/A	N/A	X
File manipulation (e.g., creation, renaming, moving)	X	N/A	N/A	N/A
Posting of any material to a PKI Repository	X	N/A	N/A	N/A
Access to the internal CA database	X	X	N/A	N/A
All Certificate compromise notification requests	X	N/A	X	X
Loading tokens with Certificates	X	N/A	X	X
Shipment of Tokens	X	N/A	X	X
Zeroising Tokens	X	N/A	X	X
Re-key of the Component	X[5]	X	X	X
CONFIGURATION CHANGES				
Hardware	X	X	N/A	X
Software	X	X	X	X
Operating System	X	X	X	X
Patches	X	X	N/A	X
Security Profiles	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing Component	X	N/A	N/A	X
Access to the Component	X	X	N/A	X
Known or suspected violations of physical security	X	X	X	X
ANOMALIES				

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

Software error conditions	X	X	X	X
Software check integrity failures	X	X	X	X
Receipt of improper messages	X	X	X	X
Misrouted messages	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X
Equipment failure	X	N/A	N/A	X
Electrical power outages	X	N/A	N/A	X
Uninterruptible Power Supply (UPS) failure	X	N/A	N/A	X
Obvious and significant network service or access failures	X	N/A	N/A	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operating System clock	X	X	X	X

5.4.2 Frequency of processing log

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

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

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

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

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

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

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

It is acceptable for the system to overwrite 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, or RA. Audit processes shall be invoked at system start-up and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records Archival

5.5.1 Types of records archived

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

Data To Be Archived	RootCA/CA	CSA	RA	CMS
Certification Practice Statement	X/X	X	X	X
Certificate Policy	X	X	X	X
Contractual obligations	X/X	X	X	X
Other agreements concerning operations of the CA	X/X	X	X	X
System and equipment configuration	X/X	X	-	X
Modifications and updates to system or configuration	X/X	X	-	X
Certificate requests	X/X	-	-	X
Revocation requests	X/X	-	-	X
Subscriber identity authentication data as per section 3.2.3	N/A / X	N/A	X	X
Documentation of receipt and acceptance of Certificates, including Subscriber Agreements	X/X	N/A	X	X
Documentation of receipt of Tokens	N/A / X	N/A	X	X
All Certificates issued or published	X/X	N/A	N/A	X
Record of Component CA Re-key	N/A / N/A	X	X	X
All CRLs and CRLs issued and/or published	X/X	N/A	N/A	N/A
All Audit Logs	X/X	X	X	X
Other data or applications to verify archive contents	X/X	X	X	X
Documentation required by compliance auditors	X/X	X	X	X
Compliance Audit Reports	X	X	X	X

5.5.2 Retention period for archive

The retention period for archive data shall depend on the legal and business requirements and is set forth in the respective CPS. However, the archive data must be kept for a

minimum retention period of ten (10) years and six (6) months, or as required by regulation. When the archive data retention time limit specified in the CPS is reached, the archived data shall be destroyed using an appropriate and irreversible method (paper shredder, disk shredder, magnetic scrambler, etc.).

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.

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

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

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

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

Key	2048 Bits		4096 Bit Keys	
	Private Key	Certificate	Private Key	Certificate
Root CAs	N/A	N/A	20 years	20 years
Sub CAs	5 years	≤ 10 years	10 years	≤ 13 years[6]
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 Signing	3 years	≤ 3 years	3 years	≤ 8 years
Code Signing or Role-Based Code Signing	10 years	≤ 10 years	10 years	≤ 10 years
Server or Device Identity or Signature	3 years	≤ 3 years	3 years	≤ 3 years
Server or Device Encryption	Unrestricted	≤ 3 years	Unrestricted	≤ 3 years
OCSP Responders	≤ 3 years	45 days	≤ 3 years	45 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

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

TSA signed by Signing CA	1 year or 500 000 signatures	≤10 years	1 year or 500 000 signatures	≤13 years

No CA shall have a private key whose validity period exceeds 20 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

5.7.1 Incident and compromise handling procedures

A formal disaster recovery plan shall exist for the Boeing Airplane Software Signing PKI Domain.

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

The Boeing Airplane Software Signing PKI PMA members shall be notified if any of the following cases occur:

- suspected or detected compromise of a Boeing Airplane Software Signing PKI CA system;
- physical or electronic attempts to penetrate a Boeing Airplane Software Signing PKI CA system;
- denial of service attacks on a Boeing Airplane Software Signing PKI CA component;
- any incident preventing a Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI PMA members shall be notified if any of the following cases occur:

- revocation of a relevant CA Certificate 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.

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 Entity Private Key compromise procedures

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

1. A new CA Key Pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
2. New CA Certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
3. The CA shall request all subscribers to re-key using the procedures outlined in section 3.3.2; and
4. If the CA is a Boeing Airplane Software Signing PKI Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI may not be a trust anchor, there are no specific requirements regarding trust anchor propagation.

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

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

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA, CMS, CSA, or RA Termination

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

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.

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 Boeing Airplane Software Signing PKI Root CA is terminated, that Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated 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
    - $2^{16} < e < 2^{256}$

6.1.1 Key pair generation

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

Entity	FIPS 140-2 Level or equivalent	Hardware or Software	Key Storage Restricted to the Module on which the Key was Generated
CA	3	Hardware	Yes
CMS	2	Hardware	Yes
RA	2	Hardware	Yes
OCSP Responder	2	Hardware	Yes
LSAP Signing	No stipulation	Hardware	Yes

Random numbers for mediumDeviceHardware-sw-parts-signing-256 Assurance Level keys shall be generated in 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. CMS Master Key and diversification master keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage issued cards.

6.1.2 Private Key Delivered to a Subscriber

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

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

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

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

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

6.1.3 Public key delivery to Certificate issuer

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

6.1.4 CA Public Key delivery to Relying Parties

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

- The CA loading a trust anchor onto tokens delivered to Subscribers via secure

mechanisms;

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

6.1.5 Key sizes

If the Boeing Airplane Software Signing PKI 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 Boeing Airplane Software Signing PKI 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	12/31/2030
	3072 or 4096 bit RSA	No stipulation
Encryption	2048 bit RSA	12/31/2030
	3072 or 4096 bit RSA	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. [7]
AES	No stipulation

All CAs shall use 2048 bit RSA, or 224 bit prime field or 233 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.

6.1.6 Public key parameters generation and quality checking

RSA keys and prime numbers shall be generated in accordance with FIPS 186-4[8].

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 Boeing Airplane Software Signing PKI 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 for Digital Signatures shall set the digitalSignature and contentCommitment bits;
- Certificates that have the contentCommitment bit set, shall not have keyEncipherment bit or keyAgreement bit set;
- Certificates to be used for encryption shall set the keyEncipherment bit;
- CA Certificates shall include cRLSign and keyCertSign bits.

Public keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure

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

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

Sockets Layer) that provide authenticated connections using Key Management Certificates and require setting both digitalSignature and keyEncipherment bits when RSA is used for the Subject's key pair.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

For PKI equipment, the relevant standards for cryptographic modules are FIPS PUB 140-2, "Security Requirements for Cryptographic Modules". The Boeing Airplane Software Signing PKI PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the Boeing Airplane Software Signing PKI PMA. Cryptographic modules shall be validated to the FIPS 140-2 or FIPS 140-3 level identified in section 6.1, or validated, certified, or verified to requirements published by the Boeing Airplane Software Signing PKI PMA; additionally, the Boeing Airplane Software Signing PKI PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

For end-entities, the relevant standard for cryptographic modules is FIPS PUB 140-2, "Security Requirements for Cryptographic Modules". However, the Boeing Airplane Software Signing PKI PMA may determine that other comparable validation, certification, or verification standards are sufficient. References to these standards will be published by the Boeing Airplane Software Signing PKI PMA in this Certificate Policy.

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.

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

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

6.2.3 Private Key escrow

Under no circumstances shall 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 medium-software-256 may be backed up or copied but must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

Human Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting an Assurance Level other than those listed above for human Subscriber shall not be backed up or copied.

Device private signature keys whose corresponding Public Key is contained in a Certificate asserting medium-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.

LSAP Signature keys whose corresponding Public Key is contained in a Certificate asserting mediumDeviceHardware-sw-parts-signing-256 Assurance Level 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.

6.2.5 Private Key archival

Private signature keys shall not be archived.

6.2.6 Private Key transfer into or from a cryptographic module

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

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

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

If a private key is transported from one cryptographic module to another, the private key must be encrypted during transport. Private keys must never exist in plaintext form outside the cryptographic module boundary.

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

6.2.7 Private Key storage on cryptographic module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 or FIPS 140-3 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).

6.2.9 Method of deactivating Private Key

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

6.2.10 Method of destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be done by overwriting the data. For hardware cryptographic modules, this usually requires executing a "zeroise" command. Physical destruction of hardware is generally not required. For CA, RA, CMS, and CSA private signature keys, the keys shall be destroyed by individuals in Trusted Roles.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and Key Pair usage periods

See section 5.6.

6.3.3 Role-Based Code Signing Keys (for signature of Aircraft software/parts)

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 id-mediumDeviceHardware-sw-parts-signing-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.

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

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

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSA, CMS, 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.

Monitoring and alerting capabilities shall be in place and described in the CPS.

When CA equipment is hosted on evaluated platforms in support of computer security

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

The CA-computer system shall be configured with the minimum number of required accounts and network services, and no remote login functionality.

Only physical hardware systems shall be used.

The Boeing Airplane Software Signing PKI Root CAs shall be operated offline with no network connections installed.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

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

- 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 authorized by local policy. CA, CMS, CSA, 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, and CMS systems as well as any modifications and upgrades shall be documented and controlled.

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

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

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

No stipulation.

6.7 Network Security Controls

The Boeing Airplane Software Signing PKI Root CA and its internal PKI Repository shall be offline.

Boeing Airplane Software Signing PKI Sub CAs, CSAs, CMS, 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.

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.

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.

Monitoring and alerting capabilities shall be in place and described in the CPS.

6.8 Time-Stamping

All CA, CSA, and CMS 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

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

Boeing Airplane Software Signing PKI CAs' critical private extensions shall be interoperable in their intended community of use.

Boeing Airplane Software Signing PKI 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. Section 10 contains the Certificate formats.

7.1.3 Algorithm object identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

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}

7.1.4 Name forms

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

Subject Name Form for CAs

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	CN	1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Required	OU	1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc"
	Required	C	1	Country name, e.g., "C=US"

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, email, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	DC	1	Domain name, e.g., "DC=xyzinc" exactly as it appears in the CA Certificate of the Issuer
	Required	DC	1…N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as it appears in the CA Certificate of the Issuer
3	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…1	<IATA Code> (Mandatory for Operators, Optional for others) Or <MMM Code> (Manufacturer's code, mandatory for Suppliers, Optional for others)
	Required	OU	1	<Customer or Supplier Name>
	Required	OU	1	"LSAP Signing Services"
	Required	O	1	"The Boeing Company"
	Required	C	1	"US"

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
4	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Required	OU	1	Boeing <Division or Function>
	Required	OU	1	"LSAP Signing Services"
	Required	O	1	"The Boeing Company"
	Required	C	1	"US"

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 Boeing Airplane Software Signing PKI CA certifies another CA within the Boeing Airplane Software Signing PKI, the certifying Boeing Airplane Software Signing PKI CA shall impose restrictions on the namespace authorized in the subordinate Boeing Airplane Software Signing PKI CA, which are at least as restrictive as its own name constraints.[9]

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

7.1.6 Certificate Policy object identifier

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

[9] This restriction shall be achieved by contractual obligations imposed onto the Subordinate CA, as well as through technical configurations on the Subordinate CA. Contracts shall identify The Boeing Company 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 The Boeing Company are enforced. The latter shall be verified through the use of monitoring software.

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

7.1.7 Usage of Policy Constraints extension

The Boeing Airplane Software Signing PKI policy domain shall follow the Certificate formats described in this CP, since inhibiting policy mapping may limit interoperability.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

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

7.2 CRL PROFILE

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

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

Section 10 contains the CRL formats.

7.3 OCSP PROFILE

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

7.3.1 Version number(s)

The version number for request and responses shall be v1.

7.3.2 OCSP extensions

Responses shall support the nonce extension.

8 Compliance Audit and Other Assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS 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

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

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 either represent a firm, which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

An example of the latter situation may be an organizational audit department provided it can demonstrate organizational separation and independence. To further ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the PKI Facility, associated IT and network systems, or certification practice statements. The Boeing Airplane Software Signing PKI PMA shall determine whether a compliance auditor meets this requirement.

In the event an entity chooses to engage compliance auditor services internal to its parent organization, it shall undergo an audit from an external third-party audit firm every third year, at a minimum.

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 Boeing Airplane Software Signing PKI PMA may determine that a CA is not complying with its obligations set forth in this CP.

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 or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Boeing Airplane Software Signing PKI PMA of the discrepancy; 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

Not applicable

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

Organizations acting as relying parties shall determine the financial limits, if any; they wish to impose for Certificates used to consummate any financial transaction. Acceptance of Boeing issued Certificates is entirely at the discretion of the organization acting as a Relying Party. Other factors that may influence the Relying Party's acceptance, in addition to the Certificate assurance level, are the likelihood of fraud, other procedural controls in place, organizational-specific policy, or statutorily imposed constraints.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

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 corporate or private information appearing in them and in public directories are not considered as private or confidential.

9.3.3 Responsibility to Protect Confidential Information

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

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

9.4 Privacy of personal information

9.4.1 *Privacy Plan*

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

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual property rights

The Boeing Company retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 Representations and warranties

Representations and warranties contained in commercial agreements between Boeing and other parties are contained in the following documents:

- Applicable Memorandums of Agreement.

9.6.1 Certification Authority Representations and Warranties

The Boeing Policy Authority authorizes the issuance and revocation of CA Certificates in particular – including self-signed and subordinate CA, for the convenience of The Boeing Company.

Boeing Airplane Software Signing PKI Certification Authorities shall agree to the following:

- The CA's signing keys are protected and that no unauthorized person has ever had access to the private keys;
- All representations made by the Certification Authority in the applicable agreements as submitted are true and accurate, to the best knowledge of the Certification

Authority;

- All information supplied by the Subscriber in connection with, and/or contained in the Certificate is true; and
- The Certificates are being used exclusively for authorized and legal purposes, consistent with this and any other applicable CP or CPS, to the best knowledge of the Certification Authority.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber representations and warranties

A Subscriber shall be required to sign a document (e.g., a subscriber agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the Certificate before being issued the Certificate.

In signing the document described above, each Subscriber shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities and other Subscribers;
- Protect their Private Keys at all times, in accordance with this policy, as stipulated in their Subscriber Agreement, and local procedures;
- Notify, in a timely manner, the OA/PMA of the CA that issued their Certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS; and
- 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.

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

None.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

A NON-BOEING SUBSCRIBER OR ENTITY SHALL HAVE NO CLAIM AGAINST BOEING ARISING FROM OR RELATING TO ANY CERTIFCIATE ISSUED BY A BOEING CA OR A CA'S DETERMINATION TO TERMINATE A CERTIFICATE. BOEING SHALL NOT BE LIABLE FOR ANY RELATED LOSSES, INCLUDING DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES.

NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL BOEING BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL, AGGREGATE LIABILITY OF BOEING FOR ALL CLAIMS ARISING OUT OF OR RELATED TO ITS IMPROPER ACTIONS SHALL NOT EXCEED ONE MILLION DOLLARS ($1 MILLION USD).

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

Termination of the CP is at the discretion of the Boeing PKI Policy Authority.

9.10.3 Effect of termination and survival

None.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

The Boeing Airplane Software Signing PKI PMA shall review this CP at least once every

year, or anytime at the discretion of the PA. Corrections, updates, or suggested changes to this CP shall be communicated to every member of the Boeing Airplane Software Signing PKI PMA, following change management procedures established by the PMA. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

After the recommended amendments or corrections to the CP have been reviewed and approved by the Boeing Airplane Software Signing PKI PMA, they shall be incorporated into the documents and public notification of the amendments shall be made through the posting of the revised CP to the Boeing externally available website.

9.12.2 Notification mechanism and period

Changes to the CP resulting from reviews and approval by the Boeing Airplane Software Signing PKI PMA are published online at http://pub.boeing.carillon.ca

This CP and any subsequent changes shall be made publicly available within ten days of approval by the Boeing Airplane Software Signing PKI PMA.

9.12.3 Circumstances under which OID must be changed

OIDs shall be changed if the Boeing Airplane Software Signing PKI PMA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute resolution provisions

Any dispute arising with respect to this policy or Certificates issued under this policy shall be resolved by the Parties.

9.14 Governing law

The construction, validity, performance and effect of Certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law or regulation).

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

10 Certificate, CRL, and OCSP Formats

This section contains the formats for the various PKI objects such as Certificates, CRLs, and OCSP requests and responses. The section only contains Certificate profiles based on RSA.

Certificates and CRLs issued under a policy OID of this CP may contain extensions not listed in the profiles in this section only upon Boeing Airplane Software Signing PKI 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 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 Self-Signed Roots (Trust Anchors)

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign
Basic Constraints	c=yes; cA=True; path length constraint absent

10.1.2 Subordinate CAs

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; keyCertSign, cRLSign
Certificate Policies	c=no; As per section 7.1.6 CPS:<URL of the public Accessible CP PDF> User Notice Explicit Text: This certificate has been issued in accordance with the Boeing Airplane Software Signing PKI Certificate Policy as found in the CPSpointer field
Basic Constraints	c=yes; cA=True; pathLength = 0
Policy Constraints	optional; c=no; inhibitPolicyMapping skipCerts = 0
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; this extension must appear in all Sub-CA Certificates and must contain at least one HTTP URI pointing to a DER encoded CRL issued by the Issuing CA. The reasons and cRLIssuer Fields must be omitted.

10.1.3 OCSP Responder Certificate

The following table contains the OCSP Responder Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the OCSP Responder Certificate.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	Issued monthly or more frequently with a validity period no longer than 45 days from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; contentCommitment, digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	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 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

10.2 End-Entity Certificates

This section describes the values that populate each field of the Certificates issued by the Boeing Airplane Software Signing PKI CAs.

10.2.1 LSAP Signing Certificate

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11}
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
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1.2.840.113549.1.1.1}
Issuer's Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (which is calculated as the SHA-1 hash of the BIT STRING subjectPublicKey, excluding the tag, length, and number of unused bits)
Key Usage	c=yes; digitalSignature, contentCommitment
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; optional; dnsName
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, must contain id-ad-ocsp access method entry with HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no; this extension must appear in all Certificates and must contain at least one HTTP URI pointing to a DER encoded CRL issued by the Signing CA. The reasons and cRLIssuer Fields must be omitted.

10.3 CRL Format

10.3.1 Full and Complete CRL

If the CA provides OCSP Responder Services, the CA shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1.2.840.113549.1.1.11}
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	sha256WithRSAEncryption {1.2.840.113549.1.1.11}
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[10], thisUpdate, nextUpdate[11],
Responder Signature	sha256WithRSAEncryption {1.2.840.113549.1.1.11}

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

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

Field	Value
Certificates	Applicable OCSP Responder Certificate
Response Extension	**Value**
Nonce	(optional) c=no; Value in the nonce field of request (only included if present in the request)[12]
Response Entry Extension	**Value**
None	None

10.6 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests.

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP.
Subject Public Key Information	Refer to section 6.1
Subject's Signature	sha1WithRSAEncryption {1.2.840.113549.1.1.5} or sha256WithRSAEncryption {1.2.840.113549.1.1.11}
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, digitalSignature, contentCommitment
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC-822, and DNS name forms

[12] 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[13]	None	None	All
OCSP Responder	id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}	None	All Others
LSAP Signing	id-kp-codesigning {1.3.6.1.5.5.7.3.3} id-eku-boeing-lsap-code-signing {1.3.6.1.4.1.73.15.3.1.42.42}	None	All Others

[13] CA Certificate includes: self-signed Root Certificate and intermediate and subordinate CA Certificates.