The Boeing Company
Medium Assurance Domain
Certificate Policy

Version 11.13

May 6, 2024

Boeing PKI Policy Authority Board approved:

May 30, 2024

Method of Approval (Roll Call / E-Mail Vote)	Date of Approval	Version Number	CR/RRs Applied
Roll Call Vote	4/7/2006	Version 7.2.1	Not applicable
Roll Call Vote and e-mail	3/8/2007	Version 8.0	
Roll Call Vote and e-mail	4/12/2007	Version 8.0.4	03-12-07-01
Roll Call Vote	7/13/07	Version 9.0	CP_CR_06-07-07_03
Roll Call Vote	9/23/08	Version 9.1	CP_CR_09-05-08_03
Roll Call Vote	1/5/09	Version 9.2	CP_CR_11_21_08_01
Roll Call Vote	3/23/09	Version 9.3	CP_CR_3_17_09_01
Roll Call Vote	11/16/09	Version 9.4	CP_CR_11_10_09_01
Roll Call Vote	1/20/12	Version 10.0	Re-write for new infrastructure
Roll Call Vote	3/1/2012	Version 10.1	CP CR 2012_01
Roll Call Vote	4/3/2012	Version 10.2	CP CR 2012_02
Roll Call Vote	5/3/2012	Version 10.3	CP CR 2012_03
Roll Call Vote	9/24/2012	Version 10.4	CP CR 2012_04
Roll Call Vote	12/14/2012	Version 10.5	MAH CP CR 2012_05
Roll Call Vote	1/11/2013	Version 10.6	MAH CP CR 2013-01
E-mail Vote	3-26-2013	Version 10.7	MAH CP CR 2013-02
Roll Call Vote	4-19-2013	Version 10.8	MAH CP CR 2013-03
Roll Call Vote	9-30-2013	Version 10.9	MAH CP CR 2013-04
Roll Call Vote	1-31-2014	Version 10.10	MAH CP CR 2014-01
Roll Call Vote	4-14-2014	Version 11.0	MAH CP CR 2014-02
Roll Call Vote	4-16-2015	Version 11.1	MAH CP RR 2015-01
E-mail Vote	4-8-2016	Version 11.2	MAH CP RR 2016-02
E-mail Vote	3-13-2017	Version 11.3	MAH CP RR 2017-01
Roll Call Vote E-mail Vote	7-21-2017 8-4-2017	Version 11.4 Section 6.1.5	MAH CP RR 2017-02
E-mail Vote Additional Changes	1-21-2019; 3-27-2019	Version 11.5	MAH CP RR 2018-01

Method of Approval (Roll Call / E-Mail Vote)	Date of Approval	Version Number	CR/RRs Applied
Roll Call Vote	4-10-2020	Version 11.6	MAH CP RR 2020-01
E-mail Vote	2-1-2021	Version 11.7	MAH CP RR 2021-01
E-mail Vote	4-12-2021	Version 11.8	MAH CP RR 2021-02
E-mail Vote	1-28-2022	Version 11.9	MAH CP RR 2022-01
E-mail Vote	4-7-2022	Version 11.10	MAH CP RR 2022-02
E-mail Vote	12-15-2022	Version 11.11	MAH CP RR 2022-03
E-mail Vote	12-19-2023	Version 11.12	MAH CP RR 2023-01
Email Vote	5-30-2024	Version 11.13	MAH CP RR 2024-01

Table of Contents

1. INTRODUCTION

The Boeing Medium Assurance Domain (BMAD) 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. These services are met with an array of network security components such as workstations, firewalls, routers, filters, proxy servers, encryption tools, and secured database and web servers. The operation of these components is supported and complemented by use of public key cryptography. Boeing does not sell certificates; rather PKI is used by the company to provide additional security to its business operations.

This Certificate Policy (CP) document defines several different policies to support the Boeing Medium Assurance Domain (BMAD). The policies represent the medium-software, medium-hardware, medium-CBP-software (Commercial Best Practice), and, medium-CBP-hardware assurance levels for public key certificates. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding the public key and the subject whose name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the subject whose name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task. The applicability statements in this policy shall be considered minimum requirements; application owners or other relying parties may require higher levels of assurance than specified in this CP.

Any use of, or reference to this CP outside the purview of the Boeing Enterprise PKI Policy 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) request for comments (RFC) 3647, CP and Certification Practice Statement Framework.

1.1 Overview

Certificate Policy (CP)

All certificates issued by Boeing Certificate Authorities contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, The Boeing Company) also publishes the CP, for examination by relying parties. Cross-certificates issued by the Boeing Principal CA (PCA) shall, in the policyMappings extension and in whatever other fashion is determined by the Boeing Policy Authority (described in section 1.3.1.1) to be necessary for interoperability, reflect what mappings exist between this CP and the cross-certified PKI CP. The affected Relying Party may use this policy mapping information to determine whether trust exists between the Boeing CA and the Relying Party’s trust anchor.

1.1.1 Relationship between the Boeing CP and the Boeing CPS

See individual CPS documents for details.

1.1.2 Scope

This CP states what assurance can be placed in a certificate issued under this policy. A PCA Certification Practice Statement (CPS) and a Subordinate CA (SCA) CPS states how the applicable certification authorities establish that assurance.

The following diagram represents the scope of the Boeing CP.

The Boeing Medium Assurance Domain (BMAD) includes the Boeing Principal CA (PCA), the Boeing Subordinate CA (SCA), the Boeing Registration Authority (RA) and the Boeing Card Management System (CMS).

The trust anchor in the Boeing CA Hierarchy is the Boeing Principal CA (PCA). This CA shall cross-certify with CertiPath.

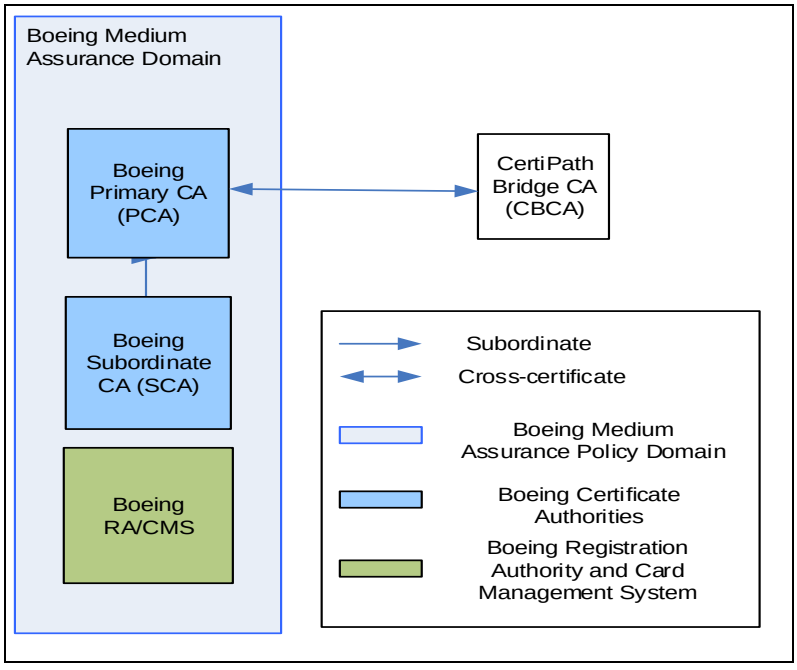
Certificates for end-entities, such as Boeing employees, are issued from the Boeing Subordinate (SCA). This CA is subordinate to the Boeing Principal CA.

The Boeing Registration Authority (RA) represents the entities responsible for identification and authentication of certificate subjects,

The Boeing Card Management System (CMS) is responsible for providing verified identities and information and manages the life-cycle of the smartcards.

Within this document, the term CA, when used without qualifier, shall refer to any certificate authority subject to the requirements of this Certificate Policy, including a Boeing PCA and a Boeing SCA. The term Boeing CA shall be used for requirements that pertain to both a Boeing PCA and Boeing SCA. Requirements that apply to a specific CA type shall be denoted by specify the CA type, e.g., Boeing PCA, Boeing SCA, etc.

Figure—Scope of Boeing CP



The scope of this CP in terms of subscriber (i.e., end-entity) certificate types is limited to those listed in applicable Certificate Profile document(s) located on http://crl.boeing.com/crl.

1.2 Document Identification

There are multiple levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an OID, to be asserted in certificates issued by the CAs that operate under this CP which comply with the policy stipulations herein.

Boeing has a Private Enterprise OID number, assigned and registered by the Internet Assigned Numbers Authority (IANA) http://www.iana.org.

The following diagram illustrates the Boeing OID structure.

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}
id-mediumSoftware-SHA256	::= {boeing-certificate-policies 11}
id-mediumHardware-SHA256	::= {boeing-certificate-policies 12}
id-mediumCBPSoftware-SHA256	::= {boeing-certificate-policies 13}
id-mediumCBPHardware-SHA256	::= {boeing-certificate-policies 14}
Id-mediumHardware-cardAuthentication-SHA256—	={boeing-certificate-policies 15}
id-mediumHardware-contentSigning-SHA256	={boeing-certificate-policies 17}

Unless otherwise stated, a requirement stated in this CP applies to all assurance levels.

The requirements associated with the Medium CBP Software (commercial best practice) Assurance policy are identical to those defined for the Medium Software Assurance policy; with the exception of personnel security requirements (see section 5.3.1).

The requirements associated with the Medium CBP Hardware Assurance policy are identical to those defined for the Medium Hardware Assurance policy; with the exception of personnel security requirements (see section 5.3.1).

The Boeing Principal CA may issue certificates to other subordinate CAs, but the subordinate CAs must assert one of the certificate policies listed above.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the CA. The PKI components identified in sections 1.3.1.5 through 1.3.1.9 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 PKI Authorities

*1.3.1.1 Boeing PKI Policy Authority (*PA) Board

The Boeing PKI PA Board is a group of individuals responsible for the direction and operation of Boeing PKIs. The Boeing PKI PA Board is responsible for:

- Commission drafting and subsequent approvals of this CP;
- Commission drafting and approval of the application for cross-certification with other authorities, such as the CertiPath Bridge Certificate Authority (CBCA);
- Reviewing the results of Certification Authority compliance audits to determine if the Certification Authorities are adequately meeting the stipulations of this CP and make recommendations to the CAs regarding corrective actions, or other measures;
- Determining the mappings, per the Boeing Operational Authority Administrator (OAA) recommendation, between certificates issued by Boeing PCAs and the levels of assurance set forth in the potential partner CPs, such as the CBCA CP (which shall include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the PA);
- After an Entity is authorized to interoperate through the Boeing PCAs, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the Boeing PCAs; and
- Approves which countries are allowed to issue Boeing Medium SecureBadge certificates and which country of citizenship is permissible for Subscriber certificate issuance.

A complete description of Boeing PKI PA Board roles and responsibilities are provided in the Boeing PKI PA Board charter.

In the event a Boeing PCA cross-certifies with another CA, Boeing shall enter into a Memorandum of Agreement (MOA) or similar instrument with an organization setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 Boeing PKI Operational Authority Members’ Group

The Boeing PKI OA Members’ Group is subordinate to the Boeing PKI PA Board and is a group of individuals responsible for:

- Practices and operations aligning to the Certificate Policy; and
- Oversight of compliant operations of PKI:

- Certification Authorities (CAs);
- Registration Authorities (RAs); and
- Infrastructure (Servers, Network, etc.).

A complete description of the Boeing PKI OA Members' Group roles and responsibilities are provided in the Boeing PKI OA Members' Group charter.

1.3.1.3 Boeing Operational Authority Administrator (OAA)

The Boeing OA Administrator (OAA), appointed by and reporting to the Boeing PA Chair, is the individual within the OA who has principal responsibility for overseeing the proper operation of the CA and its repositories.

1.3.1.4 Boeing Operational Authority (OA)

The Boeing OA operates the Boeing PCAs, the Boeing SCAs, the Boeing Registration Authority (RA) and the Boeing Card Management System (CMS). Its duties include all operations required to issue medium assurance hardware certificates from the Boeing SCAs, posting these certificates and Certificate Revocation List (CRLs) into the repository, and ensuring the availability of the repository to all relying parties. The Operational Authority acts upon approval of the Boeing PKI OA Group Members and when applicable the Boeing PKI PA Board.

The OA activities are subject to review by the Boeing PKI PA Board and/or Boeing PKI OA Group Members in order to ensure compliance with this CP and an applicable CPS.

1.3.1.5 Boeing Principal CA (PCA)

A Boeing Principal CA is a root CA operated by the OA that is designated to cross-certify directly with the CertiPath Bridge CA through the exchange of cross-certificates. A Boeing PCA is authorized by the PA to create, sign and issue public key certificates to a Boeing Subordinate CA to issue subscriber certificates under this Certificate Policy.

1.3.1.6 Boeing Subordinate CA (SCA)

A Boeing SCA is a subordinate CA in the Boeing PKI hierarchy subject to this Certificate Policy. It operates under a Boeing PCA. A Boeing SCA is authorized by a Boeing PCA to issue subscriber certificates. As operated by the OA, an SCA is responsible for all aspects of the issuance and management of a certificate including:

- The certificate manufacturing process;
- Publication of certificates;
- Revocation of certificates;
- Re-key of signing material; and
- Ensuring that all aspects of an SCA services, operations, and infrastructure related to certificates issued are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Certificate Status Authority (CSA)

A CSA is an authority that provides status of certificates or certification paths. A CSA can be operated in conjunction with an Entity's CAs or independent of the CAs. Examples of CSA are:

- OCSP Responders that provide revocation status of certificates; and
- Simple Certificate Validation Protocol (SCVP) Servers[1] that validate certifications paths 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 adhere to the same security requirements as repositories.

1.3.1.8 Card Management System (CMS)

A CMS is responsible for managing the life-cycle of a smartcard token. The CMS performs its function in accordance with a CPS approved by the OA. The Boeing OA shall ensure that the CMS associated with the Boeing SCA meets the requirements described in this CP. The CMS is responsible for all aspects of issuance, revocation and key recovery of the token content.

1.3.1.9 Registration Authority (RA)

The Registration Authority for the Boeing SCA is accomplished by a Trusted Agent interfacing with the CMS for the following functions:

- Recording the identification and authentication process required for the CMS and SCA to process the certificate request;
- Controlling certificate issuance and unlocking blocked subscribers Medium Assurance SecureBadge (MA SB) pins; and
- Interfacing with the CA for certificate issuance and revocation.

1.3.1.10 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. Subscribers include all organizational personnel. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.1.11 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 whether or how to check the validity of the certificate by checking the appropriate certificate status

[1] There are three types of SCVP Servers: path development, path validation with revocation checking, and path validation without revocation checking. The path development servers are not considered within the scope of this policy since the corruption of these servers does not adversely impact security and hence they need not be subject of a CP.

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 CP identifiers) to determine the suitability of the certificate for a particular use.

1.3.1.12 Boeing PKI Change Board

The Boeing PKI Change Board is responsible for tracking requests to create or enhance PKI products or services.

1.3.1.13 Administration Workstation

Administration Workstations may be used to administer CA, RA, CMS, and CSA equipment and/or associated HSMs from a specific secure location inside or outside the security perimeter of the CA, CMS, and CSA. In essence, the secure location housing the Administration Workstation is a logical extension of the secure enclave in which the CA, KRS, CMS, and CSA equipment resides.

1.3.2 Other Participants

1.3.2.1 Related Authorities

The CAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The applicable CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.2.2 Trusted Agent

A Trusted Agent is appointed by the OA to collect and verify each subscriber's identity information. Information shall be verified in accordance with section 3.2 and communicated to the CMS in a secure manner before the Trusted Agent encodes a subscriber's certificates onto a Boeing Medium Assurance Hardware SecureBadge. This function is further described in section 1.3.1.9.

1.3.2.3 PKI Sponsor

This CP allows for the use of PKI Sponsors in the following circumstances:

- "The Boeing Company" could be a sponsor for a human subscriber for an antecedent relationship (refer to 3.2.3.3); or
- A "human subscriber" could be a "role" sponsor for a role certificate (refer to 3.2.3.4).

1.3.2.4 Key Recovery Agents

A KRA is an individual who, using a two-party control procedure with a second KRA is authorized to interact with the KED in order to extract an escrowed key to satisfy an Administrative Key Recovery request. The Boeing Key Recovery system does not implement a "KRA" role but rather two roles: A Key Recovery Officer (KRO) and a Key Recovery Requester (KRR).

1.3.3 Applicability

The sensitivity of the information processed or protected using certificates issued by Boeing CAs varies significantly. Relying Parties must evaluate the environment and its 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 for the assurance levels 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
Medium-software or Medium-CBP-software	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in software at this assurance level.
Medium-hardware or Medium-CBP-hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware such as a smartcard or a hardware secure device, at this assurance level.

1.3.3.1 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 shall 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 PA or the Boeing Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth herein, which Relying Parties may consider in making their decisions.

1.3.3.2 Obtaining Certificates

This CP requires Boeing to publish and provide access to CA certificates and CRLs. This CP imposes no requirements in terms of publication and access to end-entity (i.e., subscriber) certificates. The Relying Party applications must make their own agreement for obtaining the subscriber certificates. This could be done for signature applications by including the signer certificate in the application protocol. For encryption applications, the Relying Party must develop a means to access subscriber certificates. Use of X.500 and LDAP Repositories is one way to achieve this, but no mechanism is mandated by this CP.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates asserting a Policy OID defined in this document shall only be used for transactions related to Boeing business in accordance with Boeing Company Policy. CAs must state this requirement in their applicable CPS and impose a requirement on Subscribers to abide by this.

1.4.2 Prohibited Certificate Uses

Certificate usage not identified in section 1.4.1 is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Boeing PKI Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact Person

The Boeing Company
Attn: Boeing PKI Policy Authority Chair, Brien Hansen
Mail Code 8J-206
PO Box 3707 Seattle, WA 98124-2207

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The applicable Certification Practice Statement (CPS) must conform to the corresponding Certificate Policy (CP). The CPS shall identify who is responsible for asserting whether the applicable Boeing Medium Level Hardware CPS conforms to the Boeing Medium Assurance Domain Certificate Policy (CP).

Determination of suitability shall be based on an independent compliance auditor's results and recommendations. The compliance auditor shall be independent from the entity being audited. The compliance auditor may not be the author of the subject CPS. The Boeing PKI PA shall determine whether a compliance auditor meets these requirements.

1.5.4 CPS Approval Procedures

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. A Boeing CPS, which is contained in a separate document published by the Boeing Operational Authority, is approved by the Boeing PKI Operational Authority Members' Group.

1.5.5 Waivers

The Boeing PKI PA does not issue waivers to CAs asserting compliance to this policy. If there is a waiver (non-compliance), it is tracked and mitigated through the non-compliance process to completion.

2. PUBLICATION AND PKI REPOSITORY RESPONSIBILITIES

2.1 PKI Repositories (Identification of Operators)

The Boeing Operational Authority (OA) shall operate repositories to support Boeing PKI operations and identify the operators in an applicable CPS.

2.2 Boeing Repository Obligations (PKI Publishing Responsibilities)

The Boeing Operational Authority may use a variety of mechanisms for posting information into PKI repositories as required by this CP. These mechanisms at a minimum shall include:

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP;
- Access control mechanisms when needed to protect repository information as described in later sections; and
- The information necessary to support interoperation of the Boeing PKI with the CertiPath Bridge CA.

2.3 Publication of Certificate Information

2.3.1 Publication of CA Information

The Boeing Operational Authority shall publish information concerning a Boeing PCA and a Boeing SCA necessary to support its use and operation.

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

The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

Each CA shall provide an online repository that is available to subscribers and relying parties and that contains:

- CA certificates asserting this policy; and
- CRLs.

The PKI Repositories containing certificates and certificate status information shall be deployed so as to provide 24 hour per day/365 day per year availability. Boeing shall implement features to provide high levels of PKI Repository reliability (99.9% availability or better).

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

CAs that provide OCSP must do so in the form of a publicly accessible delegated OCSP service, as described in Section 2.6 of RFC 6960. OCSP services must be designed and implemented to provide 99% availability or better, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

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

2.3.2 Certificate Policy Publication

A copy of this Certificate Policy shall be publicly available on the Boeing website (see http://crl.boeing.com/crl/).

The independent third-party Annual Audit Opinion Letter for The Boeing Company CA may be publicly available on http://crl.boeing.com/crl/ or a copy requested from The Boeing Company Policy Authority Chair; refer to section 1.5.2 for contact information.

2.4 Time or Frequency of Publication

Certificate Policy updates (revisions) must be published as stipulated in section 9.12.2 of this CP.

Certificates and certificate status information shall be published as specified in this CP in section 4.9.

2.5 Access Controls on PKI Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected. CA public keys and certificate status information in the Boeing PKI Repository shall be publicly available through the Internet.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A CA that asserts the policy outlined in this CP shall generate and sign certificates that contain X.500 Distinguished Names (DN) in the issuer and subject fields. The X.500 DN may also contain domain component elements. Certificates may additionally assert one or more alternate names in the Subject Alternative Name field if the field is marked non-critical.

3.1.1.1 Subject Names

For Subscriber certificates, the subject DN shall either contain the value “Unaffiliated” in the last organizational unit (ou) attribute or shall contain the affiliated organization name in the appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc)).

3.1.1.2 Subject Alternative Names

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

3.1.2 Need for Names to Be Meaningful

The identity 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 must meaningfully identify the assigned subscriber.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). The CA shall use DNs in certificates it issues. When DNs are used, the common name must respect name-space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in section 3.1.3.

All DNs shall accurately reflect organizational structures. The Subject Name in a CA certificate must match the Issuer Name in certificates it issues.

The CAs asserting one or more of the policies in this CP shall only sign certificates with subject names from within a name-space approved by the Boeing PA.

3.1.3 Anonymity or Pseudonymity of Subscribers

The Boeing CA shall not issue anonymous certificates. Pseudonymous certificates may be issued by a Boeing CA to support internal operations. CA certificates issued by a Boeing PCA shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms:

- Must use appropriate industry accepted standards (e.g., X.500, RFC822, RFC4111); and

- Must be clarified in a certificate profile.

The Boeing Operational Authority (OA) shall be the authority responsible for CA name control space.

3.1.5 Uniqueness of Names

Name uniqueness across the Boeing domains—including cross-certified domains shall be enforced. The CA and RAs shall enforce name uniqueness within the X.500 name space, for which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the PKI is ensured. The Boeing Operational Authority Administrator (OAA) shall be responsible for ensuring name uniqueness in certificates issued by the Boeing CAs.

The Boeing CA shall document in its applicable CPS:

- Which name forms shall be used; and
- How CAs and RAs shall allocate names within the subscriber community to guarantee name uniqueness among current and past subscribers (e.g., if “Joe Smith” leaves a CA’s community of subscribers, and a new, different “Joe Smith” enters the community of subscribers, how shall these two people be provided unique names?).

3.1.6 Recognition, Authentication, and Role of Trademarks

The Boeing Company will not knowingly use trademarks in names unless the subject has the rights to use that name.

3.1.7 Name Claim Dispute Resolution Procedures

The Boeing PKI PA shall resolve any name collisions brought to its attention that may affect interoperability.

3.2 Initial Identity Validation

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 CA. The CA shall then validate the signature using the party’s public key. The PA may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of Organization Identity

Requests for CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The PA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. Afterwards the PA shall direct the CA to issue a certificate to an organization.

3.2.3 Authentication of Individual Identity

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

In addition to the processes described below, Subscriber certificates may be issued on the basis of an electronically authenticated request using a valid signature or authentication certificate and associated private key, with the following restrictions:

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

This electronic authentication process does not remove the requirement for in-person identity proofing.

3.2.3.1 Authentication of Human Subscriber Identity

For subscribers, identity shall be established by in-person or supervised remote identity[2] proofing before the Trusted Agent who shall ensure that the subscriber's identity information is verified and checked in accordance with this CP and the applicable CPS. In the event an applicant (subscriber) 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. The RA shall ensure that the applicant's identity information and public key are 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 and authentication requirements shall include the following:

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

[2] Supervised Remote Identity proofing must be implemented in a manner that conforms to section 5.3.3.2 of NIST SP 800-63A *Digital Identity Guidelines: Enrollment and Identity Proofing,* dated June 2017. Future changes to NIST SP 800-63A will be reviewed for consideration.

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

- To provide proof of the country of citizenship, the applicant shall present one valid and current National Government-issued photo ID (e.g., passport, naturalization papers, certificate of citizenship), or two valid non-National Government IDs, (e.g., birth certificate) plus a recent photo ID (e.g., valid and current Driver's License). To provide their organizational affiliation, the applicant must present their Boeing badge with photo imprint;
- Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant or, in the case of electronic authentication, the serial number, subject key identifier, public key, or other unique identifier from the certificate used to authenticate the request;
- The 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, below) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration 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.

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.

Identity shall be established by in-person proofing before the Trusted Agent; information provided shall be verified to ensure legitimacy. 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

Not applicable.

3.2.3.3 Human Subscriber Re-Authentication

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

The subscriber shall present one valid National Government-issued photo ID (e.g., passport) or valid non-National Government issued photo ID (e.g., Driver's License). To provide their organizational affiliation, the applicant must present their Boeing Badge with photo imprint.

The applicable CA or RA shall ensure that the subscriber's identity information and public key are properly bound. Additionally, the CA or 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 and authentication requirements 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 this 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 equivalent and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

The process documentation and authentication requirements may include a good fingerprint match 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.

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. This CP also requires that when a certificate's private key is compromised, the derivative certificates (i.e., certificates issued on the basis of the compromised certificate) be also revoked.

3.2.3.4 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

The following requirements shall apply when human subscriber identity is verified using an antecedent relationship with a Sponsor:

- The Sponsor shall have an established relationship with The Boeing Company.

- The Sponsor shall have an established working[3] relationship with The Boeing Company sufficient enough to enable the RA to, with a high degree of certainty, verify that the Subscriber is the same person that was identity proofed by the sponsor. An example to meet this requirement is when the Subscriber and Trusted Agent are employed by the same company or a Subscriber is contracted to Boeing and a Boeing company-issued badge forms the basis for the Subscriber authentication;
- The Subscriber shall present a valid Boeing Company issued badge. This photo ID shall have been issued on the basis of in-person identity proofing using one valid Federal Government-issued photo ID (e.g., passport), or two valid Non-Federal Government I.D.s, one of which shall be a photo ID (e.g., driver's license);
- The Sponsor shall provide a signed statement to the TA containing the following information:
    - His/her own identity;
    - Date of original identity proofing event;
    - A description of the ID documents provided during the antecedent identity proofing process. These documents must satisfy the requirements in section 3.2.3.1 of this CP;
    - Historical artifacts associated with the antecedent event, if any; and
    - The name, date of birth, and other personal information that bind the individual to the identity.
- Exchange of information between the Sponsor, the Subscriber, and the TA directly pertaining to the antecedent issuance process shall be secure, and the information shall be validated, protected, and securely exchanged.
- The TA shall use the Subscriber information provided by the Sponsor to establish contact with the Subscriber.
- The Subscriber shall present a valid Sponsor-issued photo ID that matches information provided by the Sponsor as proof of identity.
- The Subscriber shall sign a declaration of identity using a handwritten signature or with appropriate digital signature using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

3.2.3.5 Authentication of Human Subscriber for Role Certificates

Subscribers may be issued role certificates. A role certificate shall identify a specific role 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. Multiple subscribers can be assigned to a role at the same time, however, the signature key pair

[3] An example of "established working relationship" is the person is employed by the Certificate Sponsor (i.e., The Boeing Company). Another example of an "established working relationship" is the person is hired as a contractor (i.e., Purchased Services personnel) of the Certificate Sponsor (i.e., The Boeing Company).

shall be unique to each role certificate issued to each individual; the encryption key pair and encryption certificate may be shared by the individuals assigned the role.

Subscribers receiving 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 the role signature certificate, the individual assigned the role or the role sponsor may act on behalf of the certificate subject for certificate management activities such as renewal, re-key and revocation. Issuance and modification of role signature certificate shall require the approval of the role sponsor. Re-key and renewal of role signature certificate shall require the approval of the role sponsor if the validity period is extended beyond that already approved by the role sponsor. For the role encryption certificate, only the role sponsor may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or RA shall record the information identified in section 3.2.3 for a sponsor associated with the role before issuing a role certificate. The sponsor shall hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role certificate. The CA or RA shall validate from the role sponsor that the individual subscriber has been approved for the role certificate.

The Role Sponsor (which is not a trusted role) shall be responsible for:

- Authorizing individuals for a role certificate;
- Recovering the private decryption key;
- Revoking individual role certificate;
- Always maintaining a current up-to-date list of individuals who are assigned the role; and
- Always maintaining a current up-to-date list of individuals who have been provided the decryption private key for the role.

3.2.4 Non-verified Subscriber Information

Unverified subscriber information shall not be included in certificates.

3.2.5 Validation of Authority

For cross-certification or issuance of subordinate CA certificates, the Boeing Operational Authority Administrator shall validate the representative’s authorization to act in the name of the organization. In addition, the Boeing OAA shall obtain the approval of the Boeing PKI PA Board prior to issuing the cross-certificate.

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

3.2.6 Criteria for Interoperation

Boeing CAs implementing this CP shall certify other CAs (including cross-certification) only as authorized by the Boeing PKI PA Board. An Entity CA shall adhere to the following requirements before being approved by the Boeing PKI PA Board for cross-certification:

- Have a CP mapped to, and determined by the Boeing PA to be in conformance with this CP; or in the case of subordinate CAs, the CA must adopt this CP and implement a CPS;
- Operate a PKI that has undergone a successful compliance audit pursuant to section 8 of this CP and as set forth in the Subject CA CP;
- Issue certificates compliant with the profiles described in this CP;
- Make certificate status information available in compliance with this CP; and
- Provide CA certificate and certificate status information to the relying parties.

3.3 Identification and Authentication for Re-key Requests

The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a Relying Party that the unique binding between a key and its named Subscriber is valid. 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 is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period.

3.3.1 Identification and Authentication for Routine Re-key

The CA and subscriber re-key requests shall be authenticated using their existing private key to sign a subscriber request or establish a client authenticated TLS session, and validated using the associated, currently valid public key certificate. Alternatively, authentication shall be accomplished by using the initial identity-proofing process as described in section 3.2.

For end-entities with medium-software, medium-CBP-software, medium hardware, and medium-CBP-hardware assurance certificates, the in-person identity-proofing process needs to be carried out once every twelve (12) years.

If it has been more than three years since a CA was identified as required in section 3.2, identity shall be re-established through the in-person registration process; see section 3.2.2.

When a current Signing key is used for identification and authentication purposes, the life of the new certificate shall not exceed beyond the identity-proofing times specified in the 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

To obtain a new certificate after a certificate has been revoked, the certificate subject shall be authenticated through use of another current, valid public key certificate in accordance with section 3.2. Alternatively, human subscriber identity may be verified

through the use of biometrics retained in the Identity Management System (IDMS) as part of the original identity proofing process.

3.4 Identification and Authentication for Revocation Request

Revocation requests shall be authenticated.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, CMS, Trusted Agent, other parties confirming identities and subscriber shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed.

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

4.1 Certificate Application

It is the intent of this section to identify the minimum requirements and procedures necessary to support trust in the PKI and to minimize imposition of specific implementation requirements on CAs, CMS, RAs, Subscribers, and relying parties.

This paragraph applies to entities seeking cross-certificates from a Boeing PCA. The Boeing PA shall establish procedures for entities to use in applying for a certificate from a Boeing CA and then publish those procedures. Additional requirements for the enrollment process for Cross-certified CAs shall be discussed in a governing agreement signed with The Boeing Company.

The Boeing Operational Authority, based on a recommendation from the Boeing PA Chair and OAA, shall act on the application and upon making a determination to issue a certificate and entering into the governing agreement with the applicant organization, shall instruct the Operational Authority to issue the certificate to the applicant CA. The applicant CA (PCA or Signing CA) shall have a distinguished name that shall be placed in the Subject field of the certificate with the common name as the official name of the CA.

For Boeing Subordinate CAs (SCA) that will be issued certificates by a Boeing PCA, the Boeing SCA shall submit an application to the Boeing PA. The application shall be, at a minimum, accompanied by a CPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647]. The PA shall evaluate the submitted CPS for acceptability. The PA may require an initial compliance analysis and pre-operational audit, performed by parties of the PA's choosing, to ensure that the CA is in compliance with this CP prior to the PA authorizing the SCA to issue and manage certificates asserting the CP.

4.1.1 Submission of Certificate Application

For certificate applications from cross-certified CAs to a Boeing PCA, the certificate application shall be submitted to the OAA by an authorized representative of the cross-certified CA.

For certificate applications to a Boeing CA, the certificate application shall be submitted to the OAA by an authorized representative of the Subject CA.

For subscriber certificates, the application shall be submitted by an authorized prospective subscriber.

4.1.2 Enrollment Process and Responsibilities

Applicants for public key certificates shall be responsible for providing accurate information in their applications.

Cross-certificates – Boeing cross-certification enrollment with CertiPath consists of:

- The Boeing OAA obtaining approval from the Boeing PKI PA Board to issue a cross-certificate to CertiPath;
- The CertiPath representative providing Boeing either a Naming Form for their issued-to-Boeing cross-certificate or the actual cross-certificate with validated information;
- The Boeing OAA (Boeing representative on the CertiPath PMA) exchanging Boeing-issued-to-CertiPath Naming Form with CertiPath to validate certificate information;
- The CertiPath representative providing a CSR for the first ever cross-certificate issuance to the OAA; subsequent cross-certificates issuances (renewals) may use the same CSR;
- The Boeing OA authorized personnel along with the OAA verifying cross-certificate attributes for accuracy before publishing or issuing and generating the cross-certificate; and
- The OAA returning the Boeing-issued-to-CertiPath cross-certificate to the CertiPath representative.

All communications supporting the certificate application and issuance process shall be authenticated and protected from modification. Cryptographic mechanisms commensurate with the strength of the private key shall be used to protect electronic communications between the RA (CMS) and CA.

4.2 Certificate Application Processing

It is the responsibility of a CA and RA to verify that the information in certificate applications is accurate. The CPS shall specify procedures to verify Information in certificate applications before certificates are issued.

4.2.1 Performing Identification and Authentication Functions

For the cross-certificate issued by the Boeing Principal CA, the identification and authentication of the applicant representing the Entity CA shall be performed by the Boeing Operational Authority Administrator.

For Boeing PCAs, the identification and authentication of the applicant representing the Boeing CA shall be performed by the Boeing Operational Authority Administrator.

For Boeing SCAs, the identification and authentication of the Subscriber must meet the requirements specified for Subscriber authentication as specified in sections 3.2 and 3.3 of this CP.

For applications by end-entities, the Trusted Agent must verify all subscriber information, in accordance with section 3.2.3. During a personal appearance, a Trusted Agent shall countersign the Subscriber agreement.

Subscribers are expected to present proof of identity in person to Trusted Agents, to agree to and sign the Subscriber Agreement.

4.2.2 Approval or Rejection of Certificate Applications

For the Boeing Principal CA, the Boeing PA may approve or reject an Entity CA certificate application.

For Boeing SCAs, the certificate may only be approved if the identity verification procedures specified in section 3.2 have been successfully completed.

4.2.3 Time to Process Certificate Applications

Certificate application processing from the time the request/application is posted on the CA or RA system to certificate issuance shall not exceed 90 days.

4.3 Issuance

Upon receiving a request for a certificate, the CA or RA shall respond in accordance with the requirements set forth in this CP and the applicable CPS.

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

While the Subscriber may do most of the data entry, it is still the responsibility of the CA and the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, 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.

4.3.1 CA Actions during Certificate Issuance

A CA shall:

- Verify the identity and authority of the requestor;
- Verify the information in the request before inclusion in the certificate;
- Generate and sign the certificate;
- Check the certificate to ensure that all fields and extensions are properly populated; and
- Post the certificate as set forth in this CP, after formal subscriber acceptance (see section 9.6.3).

4.3.2 Notification to Subscriber of Certificate Issuance

A CA shall notify a subject (e.g., CertiPath CA or Subscribers) of certificate issuance.

4.4 Certificate Acceptance

The governing agreement shall set forth responsibilities of all parties before the Boeing PA authorizes issuance of a cross-certificate by a Boeing CA. Once a CA certificate has been issued, its acceptance by the subject shall trigger the Subject CA's obligations under the governing agreement and this CP.

End-entity subscribers shall accept the responsibilities defined in section 9.6.3 by signing the Subscriber agreement during certificate issuance.

4.4.1 Conduct Constituting Certificate Acceptance

For External CAs cross-certified with Boeing PCA, certificate acceptance shall be governed by the governing agreement between Boeing and the representatives of the cross-certified CA.

For Boeing CAs operating under this policy, notification to the CA shall constitute acceptance, unless the CA objects. In the case of objection, the certificate shall be revoked.

For SCAs operating under this policy, notification to the CA shall constitute acceptance, unless the CA objects. In the case of objection, the certificate shall be revoked.

For end-entities, downloading of the certificate constitutes acceptance of the issued certificate.

4.4.2 Publication of the Certificate by the CA

The OA may use a variety of mechanisms for posting information into a repository as required by this CP. All CA certificates shall be published in a PKI Repository accessible over the Internet. There is no stipulation regarding publication of Subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Boeing OAA shall inform the Boeing PKI PA Board and Boeing PKI OA Group Members of any CA certificate issued by the Boeing Principal CA.

For the Boeing Principal CA, the OAA shall notify the CertiPath PMA of successful cross-certificate issuance.

Notification of CA certificate issuance by Boeing shall be provided to the CPMA.

End-entity CAs are not required to provide notification of certificate issuance to other entities.

In the event an SCA renews or re-keys a certificate without interaction with the RA (CMS) system involved in the existing certificate’s issuance, the CA must notify the RA (CMS) system of the action taken.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers and CAs shall protect their private keys from access by other parties at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.

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.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shoulduse public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.). In addition, relying parties should perform certificate validation in conformance with the full set of requirements specified in X.509.

4.6 Certificate Renewal

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

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

4.6.1 Circumstance for Certificate Renewal

Certificates under this CP may be renewed if:

- The certificate has not reached the end of its validity period;
- The associated private key has not been revoked or compromised;
- Certificate subject information and attributes remain unchanged;
- Validity period of the new certificate does not exceed the remaining lifetime of the private key as specified in section 5.6;
- Identify proofing requirements listed in section 3.3.1 are met;
- Information to be included in the certificate is verified to still be accurate; and
- CA certificates and Delegated OCSP responder certificates aggregated lifetime of the private key does not exceed the requirements specified in section 5.6.

4.6.2 Who May Request Renewal

Certificate requests may be made by:

- The Boeing Operational Authority Administrator or the Policy Authority chair may request renewal of cross-certificates;
- A subject may request the renewal of its certificate;
- TAs acting on behalf of the Subscriber; or
- CAs may request renewal of its subscriber certificates (e.g., when the CA re-keys).

4.6.3 Processing Certificate Renewal Requests

The following steps may be performed in any order that does not compromise security and must be completed before submitting the certificate renewal request. The procedure:

- SHALL confirm certificate satisfies the circumstances for renewal;
- SHALL authenticate the requestor using credentials whose level of assurance is at or above the certificate being renewed;
- SHALL protect the submitted information and key pair from modification;
- SHALL protect the confidentiality of shared secrets and personally identifiable information;
- SHALL ensure the requestor is authorized to submit certificate renewal requests;
- SHALL ensure the requestor agrees to be bound by a relevant Subscriber Agreement that contains representations and warranties; and
- SHALL re-use the existing key pair of the certificate.

The procedure for processing certificate renewals:

- SHALL verify the accuracy of certificate renewal request;
- SHALL verify all certificate attributes, other than the validity period and serial number, are unchanged;
- SHALL ensure the trustworthiness of the requestor;
- SHALL obtain any required approvals;
- SHALL not process any unverified certificate renewal request;
- SHALL not process any certificate renewal request that will reduce the overall level of assurance;
- SHALL not process any rejected certificate renewal request;
- SHOULD provide the reason for rejection to the requestor; and
- SHALL complete the procedure within 90 days from the time of certificate renewal request submittal.

Upon receiving a request for an approved renewal, the CA:

- SHALL authenticate the requestor using credentials whose level of assurance is at or above the certificate being requested;
- SHALL ensure the requestor is authorized to submit certificate application requests;
- SHALL verify the integrity of the information in the certificate request;
- SHALL check to ensure that all required fields and extension are properly populated;
- SHALL sign and issue a certificate if all certificate requirements have been met;
- SHALL provide the certificate to the requestor;

- SHALL NOT renew a certificate if the above cannot be completed;
- SHALL NOT renew as a certificate as a result of CA key compromise, unless the CA or CMS can verify all certificates issued since the date of compromise were issued appropriately. If the certificate cannot be verified, it must not be renewed; and
- SHOULD revoke the old certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

A CA or a representative acting on its behalf:

- SHALL inform the requestor of the certificate issuance; and
- Should instruct the requestor how to obtain the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificates shall be considered accepted if at least one of the following occurs prior to use:

- The requestor fails to object to the certificate or its contents;
- The requestor takes possession of the certificate; or
- If an authorized agent of an organization formally accepts the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

The CA or a representative acting on its behalf:

- SHALL publish appropriate certificates to repositories as necessary.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The CA or a representative acting on its behalf:

- SHALL notify the RA of certificate issuance;
- SHALL notify the Boeing PKI Policy Authority Board of root certificate issuance;
- SHALL notify the Boeing PKI Policy Authority Board of cross-certificate issuance; and
- SHALL notify the authorized agent of an organization of cross-certificate issuance.

4.7 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and 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 certificate re-key, the old certificate may or may not be revoked, but must not be used for requesting further re-key or renewals.

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.

4.7.3 Processing Certificate Re-Keying Requests

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

- In-person registration process as described in section 3.2; or
- Identification and Authentication for Re-key as described in section 3.3.

For cross-certificates issued by a Boeing PCA, certificate re-key also requires that a valid MOA exists between the Boeing PCA and the Subject CA, and the term of the MOA is beyond the expiry period for the new certificate.

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

A Boeing SCA shall not permit modifications to existing Subscriber certificates. Further, if an individual's name changes (e.g., due to marriage), then the Subscriber must enroll for a new certificate after presenting identification to support the name change.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who may request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

Revocation requests must be authenticated.

Boeing shall notify the CPMA at least two weeks prior to the revocation of a CA certificate, whenever possible.

For emergency revocation, CAs shall follow the notification procedures in section 5.7.

4.9.1 Circumstances for Revocation of a Certificate

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 becomes invalid before the certificate expires;
- The subscriber's employment is terminated or Subscriber is suspended for cause;
- The subscriber can be shown to have violated the stipulations of their subscriber agreement;
- The private key is suspected of compromise;
- The subscriber or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked; and
- Any system failure that results in loss of synchronization between BSB and MyID thus requiring manual revocation of Subscriber certificates.

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

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

4.9.2 Who Can Request Revocation of a Certificate

Any Boeing SCA certificate may be revoked upon direction of the Boeing Policy Authority. In the case of cross-certified CAs, the certificate shall be revoked upon

direction of the Boeing PA at the request of an official or officials identified in the governing agreement as authorized to make such a request.

Within the PKI, a CA may summarily revoke certificates within its domain. A certificate subject, human supervisor of a human subject, Human Resources (HR) person for the human subject, Certificate Manager, issuing CA, CMS or RA may request revocation of a subscriber certificate. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber if the CA is required to revoke all certificates within this domain.

Note that a Boeing PCA may always revoke a cross-certificate it has issued to any CA external to Boeing's policy domain.

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). In the event of a system failure requiring the manual revocation, the Certificate Manager should send an e-mail to the Boeing OAA requesting permission to revoke subscriber certificates for reasons of "system failure".

Any CA may unilaterally revoke another CA certificate it has issued. However, the Boeing OA for a Boeing CA shall revoke a Subject CA certificate only in the case of an emergency. Generally, the certificate shall be revoked based on the subject request, authorized representative of subject request, or Boeing PKI PA Board or Boeing PKI OA Group Members' 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 CA, the Boeing OA shall seek guidance from the Boeing PKI PA Board and/or Boeing PKI OA Group Members before revocation of the certificate except when the Boeing PKI PA Board or Boeing PKI OA Group is not available and there is an emergency situation such as:

- Request from the CA for reason of key compromise;
- Determination by the Boeing Operational Authority that a Subject CA key is compromised; or
- Determination by the Boeing Operational Authority that a Subject CA is in violation of the CP or its CPS to a degree that threatens the integrity of the Boeing PKI.

For cross-certified CA, the Boeing PA Chair shall direct the Boeing OA in writing to revoke the CA certificate. Upon revocation of the certificate, the OA shall post an updated CRL to the appropriate repository, in accordance with section 2.3.1.

At the medium-hardware, medium-CBP-hardware assurance levels, a Subscriber ceasing its relationship with an 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 zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time within which CA Must Process the Revocation Request

A Boeing PCA shall process all revocation requests within six hours of receipt of request.

For Subordinate CAs, revocation request processing time shall be as specified below:

Assurance Level	Processing Time for Revocation Requests
All Medium Assurance	Before next CRL is generated unless request is received within 2 hours of CRL generation

4.9.6 Revocation Checking Requirements 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 CP. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA shall ensure that superseded certificate status information is removed from the PKI Repository upon posting of the latest certificate status information.

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

The following table provides CRL issuance frequency requirements for medium-software, medium-CBP-software, medium-hardware, and medium-CBP-hardware assurance certificates.

	CRL Issuance Frequency
Routine	CAs that are off line and do not issue end-entity certificates except for internal operations must issue CRLs at least monthly; at least once every 24 hours for all others
Loss or Compromise of Private Key	Within 18 Hours of Notification
CA Compromise	Immediately, but no later than within 18 hours after Notification

The CAs that issue routine CRLs less frequently than the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs. Such CAs shall also be required to notify the Boeing OAA and PA Chair upon Emergency CRL issuance. The Boeing OAA or PA Chair shall in turn notify the CertiPath Operational Authority. This requirement shall be included in the AGREEMENT (MASTER SERVICES AGREEMENT) between CertiPath and The Boeing Company.

For offline Root, 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 168 hours.

4.9.8 Maximum Latency of CRLs

For online CAs, CRLs shall be published within 4 hours of generation.

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

4.9.9 On-line Revocation Availability

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

If on-line revocation/status checking is supported by a CA, 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 section 4.9.7.

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 of 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.

4.9.12 Special Requirements Related to Key Compromise

None beyond those stipulated in section 4.9.7.

4.9.13 Circumstances for Suspension

Boeing CAs operating under this policy do not support certificate suspension.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

Boeing CAs are not required to use certificate status services such as SCVP.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA certificates shall always be revoked at the end of subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall a CA or end user signature key be held in trust by a third party.

This CP requires a Boeing SCA to escrow decryption private keys (see section 6.2.3). Boeing key escrow and recovery capability shall be governed by the CertiPath Key Recovery Policy (KRP). The method, procedures and controls which will apply to key

recovery shall be described in a Key Recovery Practice Statement (KRPS) that has been paired with the KRP.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

This CP neither requires nor prohibits a Boeing SCA to have the capability of recovering session keys. If session keys are recoverable, a Key Recovery Policy (KRP) and a Key Recovery Practices Statement (KRPS) shall be developed.

5. FACILITY MANAGEMENT AND OPERATIONS CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The location and construction of the facility housing CA, CMS, AW, and CSA 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 CA, CMS, RA, AW and CSA equipment and records.

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA, CMS, AW, and CSA Equipment

Equipment shall always be protected from unauthorized access, especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering, including the Administration Workstations, even when the cryptographic module is not installed and activated. At a minimum, the physical access controls shall:

- Ensure that no unauthorized access to the hardware is permitted;
- Ensure that 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 (refer to 5.4 for inspection [audit] requirements); for the CSA, and specifically non-HSM related material, provide *capability* of access log review;
- Provide at least three layers of increasing security (e.g., perimeter, building, and equipment room);
- Require two-person physical access control to:
    - Both the cryptographic module and computer system for CAs and CMSs;
    - Administration Workstations (AWs);
- Require two-person control to issue the Boeing MAH OCSP Response Signing Certificate;
- Removable cryptographic modules shall be deactivated before storage;
- When not in use, removable cryptographic modules and the activation information used to access or enable cryptographic modules shall be placed in secure containers; and
- Cryptographic module activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module or any

removable hardware associated with the Administration Workstation as asserted in section 6.4.2, Activation Data Protection, of the CPS.

A security check of the facility housing CA, CMS, AW and CSA 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,” and for a PCA, that all equipment other than the repository is shut down);
- Any security containers (e.g., safes, file cabinets, physical key management systems) 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 after ensuring that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the 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

The CA shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The CA directories (containing CA-issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to support a smooth shutdown of the CA operations.

5.1.4 Water Exposures

CA, CSA, CMS, RA, and Administration Workstation equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

CA, CSA, CMS, RA, and Administration Workstation equipment shall be installed such that the possibility of fire is minimized. Boeing buildings shall have equipment in place to help with fire prevention and suppression (e.g., temperature and smoke detectors,

alarms, and suppression systems appropriate for computer equipment). Operating material (e.g., media, HSM cards, keys [cryptographic, rack]) shall be stored such that it is protected from fire based on risk acceptance.

5.1.6 Media Storage

CA, RA, and CMS media shall be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic), theft, and unauthorized access. Media that contain audit, archive, or backup information shall be duplicated and stored in locations separate from the CAs.

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

Full CA and RA backups, sufficient to recover from system failure, shall be made on a period schedule described in the applicable CPS.

Offline CA backups: In the event configuration changes or certificate issuance/revocation are made, the backup must be stored off site as soon as feasible; otherwise routine backups may be retained on site for up to 6 months, at which time the latest backup must be stored off site.

Online CA and RA backups: Backups shall be performed and then stored offsite not less than once every 7 days.

The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA and RA. The offsite backup Data Center is separate from the production CA and RA region.

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 will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. 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 (*Note*: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):

- Administrator—authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys;
- Officer—authorized to request or approve certificates or certificate revocations;
- Audit Administrator—authorized to view and maintain audit logs; and

- Operator—authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 CA Administrator

This role oversees the administration and operations of the Certificate Authority. A CA Administrator:

- SHALL design, install, configure and support CAs and the CSA;
- SHALL establish and maintain CA accounts;
- SHALL manage CA certificates, profiles and templates;
- SHALL generate CAs' and CSA keys;
- SHALL obtain/provide OCSP signing certificates;
- SHALL ensure availability and recovery of CAs, the CSA, and their keys and service accounts; and
- SHALL assist with CA and CSA monitoring and auditing.

5.2.1.2 Database Administrator

This role oversees the administration and operations of databases used for components such as the CA, monitoring solutions, or RA. A Database Administrator (DBA):

- SHALL design, implement, and operate the database;
- SHALL manage database accounts and privileges;
- SHALL define monitoring requirements for the database;
- SHALL respond to database alerts;
- SHALL analyze database alerts for trends and implement improvements as required;
- SHALL ensure availability and recoverability of databases (e.g., fault tolerance, backups, disaster preparedness);
- SHALL provide database logs required to satisfy audit requirements; and
- May provide technical support for databases.

5.2.1.3 IT Systems Administrator (IT/SA)

This role oversees the administration and operations of physical and virtual servers. An IT System Administrator:

- SHALL implement and operate server hardware;
- SHALL install, configure, and maintain server virtualization software;
- SHALL install, configure, and maintain operating systems software;
- SHALL install, configure, and maintain server security software (e.g., monitoring, anti-virus);
- SHALL manage domain and server accounts and privileges;

- SHALL manage operating system logs;
- SHALL define monitoring requirements for servers;
- SHALL respond to server alerts;
- SHALL analyze server alerts for trends and implement improvements as required;
- SHALL ensure availability and recoverability of servers (e.g., fault tolerance, backups, disaster preparedness);
- SHALL provide server data required to satisfy audit requirements; and
- SHALL provide technical support for servers.

5.2.1.4 Monitoring Systems Administrator—M/SA

A Monitoring System Administrator (M/SA) is responsible for MAH monitoring components and:

- SHALL configure and maintain monitoring software on all MAH system components;
- SHALL manage monitoring database accounts and privileges; and
- SHALL provide reports for monitoring and audit requirements.

5.2.1.5 Network Administrator

This role oversees the administration and operations of network hardware (e.g., firewalls, routers, switches) directly supporting the PKI environment. A Network Administrator:

- SHALL design, implement, and operate network hardware;
- SHALL design and implement network flow controls (e.g., routing tables, firewall rules);
- SHALL manage network hardware accounts and privileges;
- SHALL define monitoring requirements for the network hardware;
- SHALL respond to network hardware alerts;
- SHALL analyze network hardware alerts for trends and implement improvements as required;
- SHALL ensure availability and recoverability of network hardware (e.g., fault tolerance, backups, disaster preparedness);
- SHALL provide network hardware logs required to satisfy audit requirements;
- SHALL provide technical support for the network hardware; and
- SHALL configure minimum required network settings during initial setup and recovery for non-network PKI Components as defined in the CPS.

5.2.1.6 Workstation Administrator

This role oversees the configuration and maintenance of Trusted and Administration Workstations. A Workstation Administrator:

- SHALL configure and maintain Trusted Workstations (see Glossary for definition);
- SHALL configure and maintain Administration Workstations;
- SHALL maintain an inventory of workstations;
- SHALL manage workstation accounts and privileges;
- SHALL coordinate workstation replacements and updates (OS, patches, packet filters) with affected trusted roles;
- SHALL ensure availability and recoverability of the workstation (e.g., fault tolerance, backups, disaster preparedness);
- SHALL define monitoring requirements for workstations;
- SHALL provide workstation logs required to satisfy audit requirements; and
- MAY provide technical user support for the workstation.

5.2.1.7 Officer – Certificate Manager

A Certificate Manager with OAA approval:

- SHALL issue and manage CA and other critical certificates;
- SHALL approve certificate profiles; and
- SHALL approve enablement/disablement of certificate templates.

5.2.1.8 Audit Administrator

The Audit Administrator:

- SHALL review, maintain, and archive audit logs;
- SHALL verify audit logs' integrity and continuity;
- SHALL inspect all audit log entries with a more thorough investigation of any alerts or irregularities in the audit logs;
- SHALL ensure analysis verifies required items in 5.4.1; and
- SHALL provide monthly documented reporting to the Boeing OAA.

5.2.1.9 Operator

When assigned, the operator role is responsible for the routine operation of CA or CMS equipment and operations such as system backups and recovery or changing recording media.

5.2.1.10 Certificate Status Authority (CSA) Roles

A CA Administrator is the role completing the CSA role and shall have the following responsibilities for the CSA: (operated independent of the MAH CA):

- Designing, implementing, and operating the CSA;
- Defining monitoring requirements for the CSA;
- Responding to CSA alerts;

- Analyzing CSA alerts for trends;
- Providing CSA data required to satisfy audit requirements and implement improvements as required; and
- Providing technical user support for the CSA.

5.2.1.11 Card Management System (CMS) Roles

A CMS shall have at least the following roles.

- A CMS Administrator who shall be responsible for:
    - Installation, configuration, and maintenance of the CMS;
    - Establishing and maintaining CMS accounts;
    - Configuring CMS application and audit parameters; and
    - Generating and backing up CMS keys.

Practice Note: A CMS Administrator may be referred to as a Registration Authority System Administrator (RA/SA).

- A CMS Audit Administrator who shall be responsible for:
    - Reviewing, maintaining, and archiving audit logs; and
    - Analysis of anomalies and monthly reporting to the Boeing OAA.

Practice Note: An Audit Administrator performs this role.

- A CMS operator who shall be responsible for:
    - The routine operation of the CMS equipment; and
    - Operations such as system backups and recovery or changing recording media.

Practice Note: An IT/SA performs this role.

5.2.1.12 Key Recovery Agents

A KRA is an individual who, using a two-party control procedure with a second KRA is authorized to interact with the KED in order to extract an escrowed key to satisfy an Administrative Key Recovery request. The Boeing Key Recovery system does not implement a “KRA” role but rather two roles: A Key Recovery Officer (KRO) and a Key Recovery Requester (KRR).

Key Recovery Officers (KRO) authenticate the Key Recovery Requester as described in section 3.2 of the KRPS. The KRO validates the KRR’s authorization and the associated case number and approves or rejects the request.

A Key Recovery Requester (KRR) is the person who requests the administrative recovery of a decryption private key and upon approval from the KRO, recovers the decryption private key to a “Key Recovery Card.”

5.2.1.13 Trusted Agent

A Trusted Agent is responsible for:

- Verifying subscriber identity, pursuant to section 3.2.3;

- Securely communicating Subscriber information to the CMS required for the CMS and SCA to process the certificate request;
- Encoding certificates on Boeing Medium Assurance SecureBadges (MA SB); and
- Unlocking a subsciber's blocked MA SB pin.

The TA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for TAs shall be explicitly described in the CPS.

5.2.2 Number of Persons Required per Task

Two or more persons are required for CAs operating under this policy for the following tasks and additional PCA and SCA private signing key and CMS master key activation multi-person controls are described in section 6.2.2 of this CP:

- CA signing key generation;
- CA signing key activation; and
- CA signing key backup.

Where multi-person control is required:

- All persons must serve in a trusted role as defined in section 5.2.1 of this CP;
- One of the persons must be an Administrator excluding an "Audit" Administrator (i.e., Audit Administrators cannot be used to achieve multi-person control); and

All roles are recommended to have multiple persons 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 or identity.

An individual in a trusted role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) authentication, where at least one factor is a hardware token (commensurate with the strength of the PKI), shall be used for log in to the remote components.

5.2.4 Roles Requiring Separation of Duties

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

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

- Individuals who assume an Officer (Certificate Manager) role may not assume an Administrator or Audit Administrator role;
- Individuals who assume an Audit Administrator role shall not assume any other role on the CA; and
- Under no circumstances shall any of the five roles perform its own compliance auditor function.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA, CMS, CSA, and RA 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 trustworthiness and integrity, and shall be subject to a background investigation.

In addition, all persons filling trusted roles shall:

- Have a favorable outcome from a background investigation;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their duties for the trusted role; and
- Be appointed in writing by an approving authority.

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

- Have been previously relieved of duties resulting from violation of trust (e.g., willful miss-handling of information or willful miss-issuance or revocations of certificates);
- Have had a security clearance revoked for reasons other than routine review and renewal decisions;
- Have been denied a security clearance, the cause for which has not be resolved and either have had a security clearance subsequently granted or they have cleared a separate (i.e., not part of a security clearance) enhanced background screening; and
- Have been convicted of a felony offense as determined by the Boeing review/adjudication team criteria.

Practice Note: In order to make the determination if a person was denied clearance or had clearance revoked for cause, it is sufficient to rely on the local Facility Security Officer (FSO) database, Joint Personnel Adjudication System (JPAS), and assertions by the person on security clearance forms.

With the exception of Trusted Agents, each person filling a trusted role shall satisfy at least one of the following requirements:

- The person shall be a citizen of the country where the CA is located; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32.

Trusted Agents shall:

- Be citizens of the country where the TA role is performed; and
- 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.

5.3.2 Background Check Procedures

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.

When a background check is *not* performed as part of a security clearance but rather from a Boeing background screening, a Boeing-approved external company performs the enhanced background screening and a Boeing-approved adjudication process is followed. The enhanced background screening shall have a Boeing-approved refresh period (not longer than every 10 years).

The background investigation includes, but is not limited to:

- Employment (past 5 years or if the person has been in the work-force for less than five years, the employment verification shall consist of the periods during which the person has been in the work-force);
- Education (regardless of the date of award, the highest post-secondary educational degree is verified);
- Place of residence (past 3 years);
- Law Enforcement (i.e., criminal conviction history [as legally reportable]) and as pre-determined by the Boeing review/adjudication team criteria; and
- References.

5.3.3 Training Requirements

The OA shall ensure that all personnel performing duties with respect to the operation of the CA, CMS, CSA or a RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CMS/CSA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this CP and CPS.

The OA shall ensure that all personnel performing RA duties receive training appropriate to the tasks they are asked to perform. Initial training includes:

- CA Subscriber requirements during personal appearance;

- Process for encoding Boeing SecureBadge with Medium Assurance Certificates;
- RA security principles and mechanisms;
- Boeing security and operational policies and procedures;
- Ethics training; and
- Incident, compromise, and non-compliant activity reporting and handling.

A record of the training completed for each individual shall be maintained by the OA.

5.3.4 Retraining Frequency and Requirements

The OA shall ensure that all individuals responsible for PKI roles shall be aware of changes in the CA, CMS, CSA, or RA operation. 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, CMS hardware or software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

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

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

5.3.6 Sanctions for Unauthorized Actions

The Boeing PA shall take appropriate administrative and disciplinary actions against personnel who have violated this policy.

5.3.7 Independent Contractor Requirements

Contract employees (i.e., Purchased Services personnel) at Boeing are held to the same functional and security criteria that apply to a Boeing Employee in a comparable position. Contract employees shall not serve in any trusted roles.

5.3.8 Documentation Supplied to Personnel

The CP, CPS, and any relevant complementary documents, such as statutes, policies, or contracts, shall be made available to trusted role personnel. Other technical, operations, and administrative documents (e.g., administrator manuals, user manuals, 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, CMSs, CSAs, RAs, and Administration Workstations (AWs). Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.4.3, Retention Period for Archive.

A statistically significant sample of security audit data since the last review shall be examined to include a reasonable search for any evidence of malicious activity. Where possible, audit record reviews should be performed using an automated process. Such reviews involve verifying that logs have not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

In addition, the event log of the Administration Workstation shall be reconciled with the event log of the corresponding CA, CMSs, and RAs.

Audit Administrators shall explain all statistically significant sample events in a report to the OAA. Actions taken as a result of these reviews shall be documented.

5.4.1 Types of Events Recorded

All security auditing capabilities of the underlying CA, CMS, CSA, AW, and RA operating system and the CA, CMS, CSA, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the following table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- Location of the event (system affected or physical location);
- Source of the event;
- A success or failure indicator where appropriate;
- The identity of any entity, object, and/or operator associated withthe event;
- Any request or action requiring the use of a private key controlled by the CA is an auditable event. If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) must be recorded; and
- The assignment of an individual to a trusted role and removal of an individual from a trusted role are auditable events and shall include the name of the authorizing official.

The Audit Administrator shall audit that security assessments (vulnerability assessments, penetration tests) are performed per the CPS.

Auditable events to be considered shall include those in the table below.

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

Auditable Event	CA	CMS	RA	AW	CSA
SECURITY AUDIT					
Any changes to the audit logging parameters, e.g., audit frequency, type of event audited	X	X	X	X	X
Any attempt to delete or modify the audit logs	X	X	X	X	X
IDENTITY-PROOFING					
Platform or CA application-level authentication attempts	X	X	X	X	X
The value of *maximum number of authentication attempts* is changed	X	X	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X	X
DATA ENTRY AND OUTPUT					
Any additional event that is relevant to the security of the CA (e.g., remote or local data entry or data export) must be documented	X	X	X	X	X
KEY GENERATION					
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X
PRIVATE KEY LOAD AND STORAGE					
The loading of Component private keys	X	X	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	X	N/A	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE					
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	N/A	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	N/A	X
CERTIFICATE REGISTRATION					
All records related to certificate request authorization, approval, and signature	X	X	X	N/A	N/A

Auditable Event	CA	CMS	RA	AW	CSA
CERTIFICATE REVOCATION					
All records related to certificate revocation request authorization, approval, and execution	X	X	X	N/A	N/A
CERTIFICATE STATUS CHANGE APPROVAL					
All records related to certificate status change request authorization, approval, and execution	X	X	N/A	N/A	N/A
PKI COMPONENT CONFIGURATION					
Any security-relevant changes to the configuration of the Component	X	X	X	X	X
ACCOUNT ADMINISTRATION					
Roles and users are added or deleted	X	X	N/A	X	N/A
The access control privileges of a user account or a role are modified	X	X	N/A	X	N/A
CERTIFICATE PROFILE MANAGEMENT					
All changes to the certificate profile	X	X	N/A	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT					
All changes to OCSP profiles (e.g., OCSP Response Signing and Format profiles)	X	N/A	N/A	N/A	N/A
MISCELLANEOUS					
Appointment of an individual to or removal from a Trusted Role including the name of the authorizing official	X	X	X	X	X
Designation of personnel for multiparty control	X	X	X	X	N/A
Installation of the Operating System	X	X	X	X	X
Installation of the PKI Application	X	X	X	N/A	X
Installation of hardware cryptographic modules	X	X	X	N/A	X
Removal of hardware cryptographic modules	X	X	X	N/A	X
Destruction of cryptographic modules	X	X	X	N/A	X
System Startup	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	N/A	X
Receipt of hardware / software	X	X	X	N/A	X
Attempts to set passwords	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X
Back up of the internal CA database	X	N/A	N/A	N/A	N/A
Restoration from back up of the internal CA database	X	N/A	N/A	N/A	N/A

Auditable Event	CA	CMS	RA	AW	CSA
Critical file manipulation (e.g., creation, renaming, moving)	X	-	-	X	N/A
Posting of any material to a PKI Repository	X	-	N/A	N/A	N/A
Access to the internal CA database	X	-	N/A	N/A	X
All certificate compromise notification requests	X	X	X	N/A	N/A
Loading tokens with certificates	X	X	X	N/A	N/A
Shipment of Tokens and receipt of Tokens from/by the component that contain key material or that allow access to key material	X	X	X	N/A	N/A
Zeroizing and Destroying Tokens	X	X	X	N/A	N/A
Re-key of the Component	X	X	X	N/A	X
CONFIGURATION CHANGES					
Hardware	X	X	-	X	X
Software	X	X	X	X	X
Operating System	X	X	X	X	X
Patches	X	X	-	X	X
Security Profiles	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY					
Personnel Access to room housing Component	X	X	-	X	-
Access to the Component	X	X	-	X	X
Known or suspected violations of physical security	X	X	X	X	X
ANOMALIES					
Software error conditions	X	X	X	X	X
Software check integrity failures	X	X	X	X	X
Equipment failure	X	X	-	-	-
Electrical power outages	X	X	-	-	-
Uninterruptible Power Supply (UPS) failure	X	X	-	-	-
Obvious and significant network service or access failures	X	X	-	-	-
Violations of Certificate Policy	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X

5.4.2 Frequency of Processing Logs

Audit logs shall be reviewed:

- Monthly for online CAs, RAs, CSAs, and Administration Workstations;
- Whenever offline CAs are activated (at least monthly);
- Whenever deemed necessary or warranted by an alarm or discovered anomalous event; and
- To recover space to prevent the log from becoming full.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained:

- And not archived off-site until reviewed; and
- For the time needed to support audit requirements.

5.4.4 Protection of Audit Logs

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

- Only authorized people have read access to the logs;
- Only authorized people may archive audit logs;
- Multi-person control is in place for managing the audit logs (e.g., collect, review, backup, rotate, delete, etc.); and
- Audit logs are not modified.

Procedures must be implemented to protect audit records from deletion or destruction. Audit logs shall be moved to a safe, secure storage location separate from the equipment they are generated on.

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

5.4.5 Audit Log Backup Procedures

Audit logs shall be backed up:

- At least monthly for online systems;
- Whenever offline CAs are activated (at least monthly);
- To an offsite location per CPS; and
- Whenever deemed necessary or warranted.

5.4.6 Audit Collection System (Internal vs. External)

The audit log generation process shall be internal to the CA, CMS, CSA, and RA. It shall run automatically without human intervention.

Audit log generation processes shall be invoked at system startup and cease only at system shutdown. The audit log generation process shall receive confirmation that audit logs are successfully stored in the audit log collection system.

The audit log collection system may or may not be external to the CA, CMS, CSA, or RA. Audit collection systems shall be configured to ensure security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, a determination shall be made by the OA whether to suspend the associated operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

Routine security assessments (e.g., vulnerability assessments, penetration tests) are performed as stipulated in the CPS.

5.5 Records Archive

5.5.1 Types of Records Archived

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

Data to Be Archived	CA	CMS	RA	CSA
Certification Practice Statement	X	X	X	X
Certificate Policy	X	X	X	X
Contractual obligations	X	X	X	X
System and equipment configuration	X	X	-	X
Modifications and updates to system or configuration	X	X	-	X
All records related to certificate request, authorization, approval, and signature	X	X	-	-
All records related to certificate revocation	X	X	-	-
Records specific to the assignment of an individual to or removal from a trusted role	X	X	X	X
Subscriber identity authentication data as per section 3.2.3	X	X	X	N/A
Documentation of receipt and acceptance of certificates	X	X	X	N/A
Documentation of receipt of Tokens	X	X	X	N/A
All certificates issued or published	X	X	N/A	N/A
Record of Component CA Re-key	X	X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents	X	X	X	X

Data to Be Archived	CA	CMS	RA	CSA
Documentation required by compliance auditors	X	X	X	X
Compliance Audit Reports	X	X	X	X

5.5.2 Retention Period for Archive

The archive retention period for records associated with a specific CA begins at CA key generation and shall be maintained for a minimum of three (3) years following CA expiration or termination.

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.

Alternatively, data may be retained using procedures that have been approved by the U.S. National Archives and Records Administration or by the respective records retention policies in accordance with applicable laws. A method shall be implemented as defined in the CPS to ensure data can be read regardless of associated application. (e.g., maintain the original/updated applications, schema of the database tables).

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

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to write to, modify, or delete the archive. Authorized individuals are either Audit Administrators or individuals who do not have access to the system the archive record is generated from and approved by the Boeing OAA.

The contents of the archive shall not be released except as determined by the Boeing PA, OAA, or as required by law.

Archive media shall be stored in a safe, secure storage location separate from the PKI components (CA, CMS, CSA, or RA) in read-only format with physical and procedural security controls. Deletion of archive records is not permitted under any circumstances prior to the end of the required retention period.

5.5.4 Archive Backup Procedures

Not applicable.

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall have accurate timestamps with sufficient precision such that the sequence of events can be determined.

The CPS shall describe how system clocks used for timestamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (internal or external)

The archive collection system may be internal or external but must be identified 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 published in the CPS.

5.6 Key Changeover

As a CA approaches the end of its validity period, planning should be put in place to ensure a smooth transition to a new CA, unless the intention is to cease certificate production.

Each CA's private key shall have a validity period no greater than the period described in the table below. Prior to the end of a CA private key's signing validity period a new CA shall be established. From that time on, only the new key shall be used to sign CA and/or subscriber certificates. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. The old private key shall continue to be used to sign CRLs and OCSP Responder certificates until the expiration of the CA certificate or expiration/revocation of all certificates issued by the CA, whichever comes first, and must be protected accordingly.

The following table provides the maximum lifetimes for certificates and associated private keys by certificate type.

Certificate Type	Private Key	Certificate
Boeing PCA G3	20 years	20 years
Boeing Medium Assurance Hardware Issuing CA G3	10 years	10 years
Boeing Medium SecureBadge Identity or Signature	3 years	3 years
Boeing Medium SecureBadge Encryption	Unrestricted	3 years
Boeing Medium SecureBadge Card Authentication	3 years	3 years
OCSP Responder	3 years	120 days

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Each organization operating an PKI component shall have a formal disaster recovery plan.

If a CA, CSA, or CMS detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA, CSA, or CMS key is suspected of compromise, the procedures outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA, CSA, or CMS needs to be rebuilt, only some certificates need to be revoked, and/or the CA, CSA, or CMS key needs to be declared compromised. If it is determined that an incident has occurred with the potential to affect the operations and/or security environments, CertiPath shall be notified within 24 hours of determination and provided a preliminary remediation analysis.

Once the incident has been resolved, the Boeing PKI PA Chair or OAA shall notify CertiPath. The notification shall provide detailed measures taken to remediate the incident and include the following:

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

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

The Boeing PA Board and all cross-certified PKIs shall be notified if any of the following cases occur:

- Suspected or detected compromise of the Boeing PKI system;
- Physical or electronic attempts to penetrate the Boeing PKI system;
- Denial of service attacks on a Boeing PKI component; or
- Any incident preventing the Boeing PKI from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The Boeing PA shall follow the process identified above to notify all cross-certified entities of the final incident resolution.

The Boeing PA Board and all cross-certified PKIs shall be notified if any of the following cases occur:

- A CA certificate revocation is planned; or
- Any incident preventing a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The above measures will allow member entities to protect their interests as Relying Parties.The Boeing OA shall reestablish 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 is 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 Corruption

If the CA, CSA, CMS, or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. Before returning to operation, ensure that the system's integrity has been restored. The Boeing PA shall be notified as soon as possible.

If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

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[4] notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties. If the ability to revoke certificates is inoperative or damaged, the CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS. If revocation capability cannot be established in a reasonable timeframe, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

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

- The CA shall request revocation of any certificates issued to the compromised CA immediately;
- A CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
- New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
- If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the notAfter date in the certificate as in original certificates; and
- If the CA is the Root CA, it shall provide the Subscribers the new trust anchor using secure means.

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

If a CSA or CMS key is compromised, all certificates issued to the CSA or CMS shall be revoked, if applicable. The CSA or CMS will generate a new key pair and request new certificate(s), if applicable.

---

[4] With confidentiality, source authentication, and integrity security services applied.

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

- The RA certificate shall be immediately revoked;
- A new RA key pair shall be generated in accordance with procedures set forth in the applicable CPS;
- New RA certificate shall be requested in accordance with the initial registration process set elsewhere in this CP;
- All certificate registration requests approved by the RA since the date of the suspected compromise shall be reviewed to determine which are legitimate; and
- For those certificates requests or approval than 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 the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the Boeing PKI PA Board shall be notified at the earliest feasible time, and the Boeing PKI PA Board shall direct the OA to revoke the CA certificates. Further, operations shall be re-established as quickly as possible by following the procedures for CA key loss or compromise detailed in section **Error! Reference source not found.** above.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending re-establishment of CA operation with new certificate.

5.8 CA, CMS, CSA, or RA Termination

In the event of a CA termination, the following shall occur:

- Boeing provides as much advance notice as circumstances permits to all cross-certified entities prior to the termination and attempts to provide alternative sources of interoperation will be sought;
- If a Root CA is terminated, the Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the CA;
- Whenever possible, notification of termination will be provided at least two weeks prior to the termination;
- The CA requests all certificates issued to it be revoked prior to termination;
- The CA, CMS, CSA, and RA archive all audit logs and other records prior to termination;
- The CA, CMS, CSA, and RA archive records shall be transferred to an appropriate authority (e.g., the Boeing OA responsible for the entity, the Boeing OAA, etc.);
- The CA, CMS, CSA, and RA shall destroy all its private keys upon termination; and
- The CPS shall further define controls for destruction of material.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140 Level	Hardware or Software	Key Storage Restricted to The Module on Which the Key Was Generated
CA	3	Hardware	Yes
CMS	3	Hardware	Yes
RA	3	Hardware	Yes
Content Signing	2	Hardware	Yes
End-Entity Signature or Authentication (medium-software and medium-CBP-software)	1	Software	No Requirement
End-Entity Encryption (medium-software and medium-CBP-software)	1	Software	No Requirement
End-Entity Signature or Authentication (medium-hardware, medium-CBP-hardware)	2	Hardware	Yes
End-Entity Encryption (medium-hardware, medium-CBP-hardware)	2	Hardware	No Requirement
Server (medium-software and medium-CBP-software)	1	Software	No Requirement
Server (medium-hardware, medium-CBP-hardware)	2	Hardware	Yes

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

Random numbers for medium-hardware and medium-CBP-hardware assurance level keys shall be generated in FIPS 140 Level 2 or higher validated hardware cryptographic modules.

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

Multiparty 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 the process were followed. The documentation of the process shall be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third-party.

Activation of the CMS master key shall require strong authentication of Trusted Roles. Key diversification operations by the CMS shall occur in the CMS hardware cryptographic module. The diversified keys shall only be stored in hardware cryptographic modules that support medium hardware. CMS master key and diversified 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 Delivery to Subscriber

A CA shall generate its own key pair and therefore does 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 signing 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); and
- 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 CMS shall maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the applicable CPS. Delivery may be accomplished by either secure electronic or non-electronic mechanisms. If offline means are used, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished. The following requirements apply:

- Where key pairs are generated by the Subscriber or CMS, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance; and
- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the subscriber key pair.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the subscribers acting as relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

- Secure distribution of a trust anchor through secure out-of-band mechanisms; or
- Downloading a trust anchor from a web site secured with a currently valid certificate and subsequent comparison of the hash of the certificate against a hash value made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism).

6.1.5 Key Sizes

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 one of the following algorithms for the time periods indicated:

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

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

Type	Name	Sunset Date
Symmetric Algorithms	Symmetric Algorithms	Symmetric Algorithms

All certificates, CRLs, and OCSP Responses shall use one of the following hash algorithms for the time periods indicated:

Type	Issued before 12/31/2030	Issued after 12/31/2030
Hashing Algorithm for Certificates	SHA-256 or SHA-384	SHA-256
Hashing Algorithm for CRLs	SHA-256 or SHA-384	SHA-256
Hashing Algorithm for OCSP Responses	SHA-256 or SHA-384	SHA-256

CRLs, OCSP Responder certificates, and OCSP Responses shall use the same or stronger signature algorithms, key sizes, and hash algorithms as used by the CA to sign the certificate in question.

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

For RSA, the PKI shall conduct public key parameters generation and quality checking in accordance with NIST SP 800-89.

For ECC, public keys shall fall within curves defined in section 7.1.3.

Additionally, the PKI shall confirm the validity of all keys as specified in NIST SP 800-56A.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is determined by the key usage and extended key usage extension in the X.509 certificate. For key usage, the following constraints shall apply:

- Certificates to be used solely for authentication shall set only the digitalsignature bit;

- Certificates to be used by human subscibers for digital signatures shall set the digitalsignature and nonrepudiation bits;
- Certificates that have the nonrepudiation bit set, shall not have the keyEncipherment bit or keyAgreement bit set;
- Certificates to be used for encryption shall set the keyEncipherment bit;
- Certificates to be used for key agreement shall set the keyAgreement bit; and
- CA certificates shall set cRLSign and CertSign bits.

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

Public keys that are bound into human subscriber certificates shall be certified for use in signing or encrypting, but not both. For end-entity certificates the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}.

The extended key usage shall meet the requirements stated in the Certificate Profile document on crl.boeing.com/crl. Extended Key Usage values shall be consistent with key usage bits asserted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140]. The Policy Authority (PA) may determine that other comparable validation, certification, or verification standards are sufficient: These standards shall be published by the Boeing PA. Cryptographic modules shall be validated to a FIPS 140-2 or higher level in section 6.1.1. Additionally, the Boeing PA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

The table in section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used. In addition, private keys shall not exist outside the cryptographic module in plaintext form.

6.2.2 Private Key Multi-Person Control

Use of a CA or CSA private signing key shall require action by at least two trusted roles as described in section 5.2.2 of this CP. Additionally, activation of a PCA and Subordinate CA private signing keys and CMS master key activation shall be HSM-enforced.

6.2.3 Private Key Escrow

Under no circumstances shall a signature key be held in trust by a third party.

Human subscriber private keys used for decryption shall be escrowed. The method, procedures, and controls that will apply to the storage, request for extraction and/or

retrieval, delivery protection, and destruction of the requested copy of an escrowed key shall be described in a Key Recovery Practice Statement.

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 used to generate and protect the original signature key as referenced (see section 5.2.2). A single copy of the signature key may be kept at the CA location; a second copy may be kept at the CA backup location; a third copy may be kept at the DR location.

All copies of the CA keys will be stored commensurate to the original CA keys. Backup procedures shall be maintained in a separate CA Operational document.

6.2.4.2 Backup of subscriber private signature key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the medium-software 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.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the medium-hardware and/or high-hardware may not be backed up or copied.

6.2.4.3 Backup of CSA Private Signature Key

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

6.2.5 Private Key Archival

Private signature keys shall not be archived.

For private encryption keys (key management or key transport), see sections 6.2.3.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys shall be generated by and remain under control of a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key shall be protected using a FIPS approved algorithm and a bit strength commensurate with the key being transported. It must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

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

Subscriber private keys used for non-repudiation must be generated by and remain in a cryptographic module. Subscriber private keys used for encryption may be generated or

escrowed outside of a cryptographic module in accordance with section 4.12 and 6.1.1.3.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store private keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140 rating of the cryptographic module.

6.2.8 Method of Activating Private Keys

Under this CP, CA signing key activation requires multiparty control as specified in section 5.2.2.

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. When passphrases or PINs are used, they shall be a minimum of six (6) characters. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For content signing certificates, the CMS may be configured to activate its private key without requiring its authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented. The strength of the security controls shall be commensurate with the level of threat in the PKI environment, and shall protect the PKI hardware, software, and the cryptographic token and its activation data from compromise.

In the event a subscriber forgets the PIN and the card is locked, s/he must appear before a Trusted Agent to have the PIN unblocked.

6.2.9 Methods of Deactivating Private Keys

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 CPS. CA, CSA, and CMS hardware cryptographic modules shall be removed and stored in a secure container when not in use as defined in section 5 in the CPS.

6.2.10 Method of Destroying Private Keys

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 hardware cryptographic tokens, this will likely be executing a “zeroize” command.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects Of Key Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

The validity period of a certificate must not exceed the lifetime of the key, as listed in section 5.6. Certificate lifetime can be found in the applicable Certificate Profile document on crl.boeing.com/crl.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock a CA, CMS, RA, CSA, or subscriber private keys, in conjunction with any other access control procedure, 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 cryptographic module used to store the keys. Subscriber activation data may be user selected. For CAs, activation data 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 be either biometric in nature or memorized (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, CMS, 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. A CA, CMS, CSA, RA, and AW shall include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control, including managing privileges of users to limit users to their assigned roles;
- Provide a security audit capability (see section 5.4);
- 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 processes;
- Provide self-protection for the operating system;
- Require self-test security related CA services (e.g., check the integrity of the audit logs); and
- Support recovery from key or system failure.

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

The computer system shall be configured with the minimum of the required accounts, software, and network services. Access other than physical access is only permitted from an approved secure location (i.e., a cross-site) using approved controls with the exception being the CSA which is accessible with authorized, secured mechanisms as stipulated in the CPS .

6.5.2 Computer Security Rating

If available, computer security rating requirements shall be identified in the CPS.

6.6 Life-cycle Security Controls

6.6.1 System Development Controls

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

- Use software that has been designed and developed under a formal, documented development methodology;
- Where open-source software has been utilized, security requirements shall be achieved through software verification and validation and structured development life-cycle management. 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);
- All hardware and software must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase to the operations location;
- Hardware and software used and/or developed specifically for a CA, RA, and CMS 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;
- 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 part 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, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter; and

- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of a CA, RA, CSA, and CMS as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism to periodically verify the integrity of the software and to detect unauthorized modification to a CA, RA, CSA, and CMS software or configuration. CA, RA, 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.

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

6.6.3 Life Cycle Security Ratings

If available, CA life-cycle security controls shall be identified in the CPS.

6.7 Network Security Controls

PCAs are never connected to a network.

CAs, CSAs, CMSs, Administration Workstations, and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of network guards, firewall, or filtering routers. Unused network ports and services shall be turned off. The network guard, firewall, or filtering router shall limit services allowed to and from the PKI equipment to those required to perform PKI functions.

Protection of PKI equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the PKI equipment shall be necessary to the functioning of the PKI application.

If the Administration Workstation is located outside the security perimeter of the CA, CMS, and CSA, it shall access the PKI Enclave using site-to-site solution such as firewall-to-firewall or router-to-router encrypted channel. The site-to-site solution shall use FIPS approved cryptography (e.g., FIPS approved algorithms housed in FIPS approved cryptographic modules) commensurate with the cryptographic strength of certificates issued by the PKI being administered. The site-to-site solution shall be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret based, the shared secret shall be changed at least annually, shall be randomly generated, and shall have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered. Alternatively, when the Administration Workstation is located inside the security perimeter of the CA, CMS, and CSA, and protected by the boundary controls of the PKI Enclave, appropriate techniques

shall be used for mutual authentication of the PKI components and mutual authentication of traffic flowing among them.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

Remote access shall be mediated by a bastion host or “jump server” (i.e., a machine that presents a limited interface for interaction). All network activity to the PKI components (e.g., CA, CMS, and/or CSA) shall be initiated from the jump server. The bastion host is considered part of the CA, CMS, and/or CSA and shall meet the security requirements for these components. A remote workstation or user shall perform mutual authentication with the bastion host using strong authentication (e.g., PKI credential) commensurate with the strength of the PKI environment. Cryptographic material derived from the authentication shall be used to protect the communication with the bastion host. (Note: client-authenticated TLS, SSH, and IPSEC are examples of protocols that meet this requirement.) In addition, the user shall authenticate to the PKI component being administered via the bastion host. In other words, authentication to the bastion host does not alleviate the need to authenticate to the PKI component(s) being administered.

Remote administration shall be designed such that there are positive controls to meet the multi-person control requirements specified in this CP, applicable KRP, CPSs, and KRPSs. Note that the KRPS requires that the KED and Key Servers be under continuous multi-person control.

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

6.8 Time Stamping

PCAs are manually synchronized against an atomic time-based source (e.g., cell phone network time).

SCA and CSA components shall regularly synchronizes time with National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol (NTP) ServiceTime 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; and
- OCSP or other CSA responses.

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see section 5.4.1.

7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

Certificate Profiles:

- SHALL be documented with specific usage and attribute values;
- SHALL be located on http://crl.boeing.com/crl; and
- SHALL be reviewed annually and updates applied as required.

7.1 Certificate Profile

7.1.1 Version Numbers

The use of version numbers shall comply with the X.509 standard defined in RFC 5280.

7.1.2 Certificate Extensions

CA certificates shall not include critical private extensions.

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

Issuer CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, The Certificate Profile document(s) contain the certificate formats.

Any optional certificate extension requests must be submitted by the Boeing OA to the Boeing OAA for approval and must be documented in the applicable CPS.

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) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha384(3)}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha512(4)}

Certificates under this CP shall use the following OID for identifying the subject public key information:

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

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with

the attribute type as further constrained by RFC5280. Subject and issuer fields shall include attributes as detailed in the table below.

For attribute values other than dc and e-mail address, all Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as printable string. If a portion cannot be encoded as printable string, then and only then shall it be encoded using the UTF-8 format.

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.

Example: CN=Boeing SecureBadge Medium G2, OU=Certservers, O=Boeing, C=US

Table 1 Subject Name Forms (CA)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content column	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities”, or similar text
	Required	O	1	Issuer name, e.g., “O=XYZ Inc”
	Required	C	1	Country name, e.g., “C=US”
2	Required	See Content column	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities”, or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyzinc” exactly as it appears in the CA certificate(s)
	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(s)

Table 2 Subject Name Form (Non-CA)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content column	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, e-mail, 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(s)
	Required	C	1	Country name, e.g., “C=US” exactly as it appears in the CA certificate(s)
2	Required	See Content column	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”
	Required	DC	1	Domain name, e.g., “DC=xyzinc” exactly as it appears in the CA certificate(s)
	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(s)

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.

7.1.5 Name Constraints

Boeing CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in a Certificate Profile subject to the requirements above.

7.1.6 Certificate Policy Object Identifier

With the exception of self-signed Root CA certificates, all CA and Subscriber Certificates shall assert one or more of the certificate policy OIDs listed in section 1.2 of this CP.

Cross-certified CAs shall not assert Boeing policy OIDs in the certificates they issue with the exception of the *subjectDomain* field in the policy mappings extension of the cross-certificate issued to Boeing.

When a CA asserts a policy OID, it may also assert all lower assurance policy OIDs.

OCSP Responder certificates shall assert all policy OIDs for which the issuing CA is authoritative.

7.1.7 Usage of Policy Constraints Extension

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

A Boeing PCA shall adhere to the Certificate Formats described in this CP and the Certificate Profiles 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, and CP and CPS pointers.

Certificates issued by cross-certified CAs may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The certificate policies extension shall not be marked critical.

7.1.10 Inhibit Any Policy Extension

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

7.2 CRL Profile

Full and complete CRLs shall be issued.

7.2.1 Version Numbers

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.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960. OCSP request and response formats can be found in Certificate Profile documents on http://crl.boeing.com/crl.

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

7.3.1 Version Number

The version number for requests and responses shall be V1.

7.3.2 OCSP Extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Boeing PKI PA Board, working through the Boeing PKI OA Group Members, shall have a compliance audit mechanism in place to ensure that the requirements of applicable governing agreements, this CP and related CPSs are being implemented and enforced.

8.1 Frequency of Audit or Assessments

All CAs, CMSs, CSAs, and RAs shall be subject to a periodic compliance audit at least once per year.

The Boeing OA shall conduct a compliance audit annually. Additionally, the Boeing PKI PA Board or Boeing PKI OA Group Members have the right to require periodic inspections of Boeing CAs and CMS to validate that they are operating in accordance with their respective CPS.

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 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 entity’s PKI Facility, associated IT and network systems, or certification practice statements. The Boeing PA 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 the applicable CP, the component CPS, and the applicable governing agreements between Boeing, CertiPath and other Entities. The compliance audit must include an assessment of the applicable CPS against the applicable 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 PA may determine that a CA is not complying with its obligations set forth in this CP or the applicable governing agreements. When such a determination is made, the Boeing PA may suspend operation of a noncompliant CA it controls, or may direct the Boeing Operational Authority to cease interoperating with the affected CA (e.g., by

revoking the cross- or subordinate certificate issued to the CA), or may direct that other corrective actions be taken which allow interoperation to continue. If the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, the governing agreements, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Certification Authority of the discrepancy. The Certification Authority shall notify the Boeing PKI PA promptly; and
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the governing agreement, 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 Boeing PA may decide to temporarily halt operation of a Boeing CA, to revoke a certificate issued by a Boeing CA, or take other actions it deems appropriate. The Boeing PA shall authorize the development of procedures for making and implementing such determinations.

8.6 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Certification Authority, shall be provided to the Boeing PA 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 Entity PKI 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 section 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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Not applicable.

9.1.1 Certificate Issuance/Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fee

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/warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality Of Business Information

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the applicable organization.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

The Boeing Company may collect, store, process and disclose personally identifiable information in accordance with The Boeing Company Personal Information Protection and Privacy Policy which designates standard methods and tools for privacy protection.

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:

- Policy Mapping Services Agreement between Boeing and CertiPath;
- Master Services Agreement between Boeing and CertiPath; and
- 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, subordinate CA, and cross-certificates for the convenience of The Boeing Company.

Boeing Certification Authorities shall agree to the following:

- The Boeing 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 (Trusted Agent) Representations and Warranties

Trusted Agents (TAs) shall represent and warrant that identity verification is performed in accordance with section 3 of this Certificate Policy.

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 or immediately following certificate issuance.

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 Agreements, and local procedures;
- Notify, in a timely manner, the OA/PA 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.

9.6.4 Relying Parties 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 the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA that issued the certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment; and
- 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. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

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 this CP is at the discretion of the Boeing PKI Policy Authority Board.

9.10.3 Effect of Termination and Survival

None.

9.11 Individual Notices and Communications With participants

Any planned change to the infrastructure of a Boeing CertiPath-related CA that has the potential to affect the CBCA operational environment shall be communicated to the CPMA at least two weeks prior to implementation, and any new CA certificates produced as a result of the change provided to the CPMA within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for Amendment

The Boeing PKI PA 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 PKI PA, following change management procedures established by the PA. 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 PKI PA Board, 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 PKI PA Board are published online at http://crl.boeing.com/crl/. In addition, changes are communicated to all cross-certified partners.

This CP and any subsequent changes shall be made publicly available within thirty days days of approval by the Boeing PKI PA Board.

9.12.3 Circumstances under which OID must be changed

OIDs shall be changed if the Boeing PKI Policy Authority 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 (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10. CERTIFICATE, CRL AND OCSP FORMATS

No further stipulation other than what is in this CP and/or the Certificate Profile document(s). The Certificate Profile documents shall represent CA and template settings. Each Boeing environment shall have unique Certificate Profile documents which contain the certificate profiles, versions, and extensions used. The Certificate Profile documents can be found on http://crl.boeing.com/crl.

11. PKI REPOSITORY INTEROPERABILITY PROFILE

This section provides an overview of the PKI Repository interoperability profiles. The following topics are discussed:

- Protocol;
- Authentication;
- Naming;
- Object Class; and
- Attributes.

Each of these items is described below.

11.1 Protocol

Boeing PKI Repositories shall provide HTTP and may provide, upon request, LDAP access to certificates and CRLs.

11.2 Authentication

Each PKI Repository shall permit “none” authentication to read certificate and CRL information.

Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc. shall require password over TLS or stronger authentication mechanism.

11.3 Naming

This CP has defined the naming convention

When an LDAP repository is used:

- Certificates shall be stored in the LDAP Repository in the entry that appears in the certificate subject name; and
- The issuedByThisCA element of crossCrossCertificatePair shall contain the certificate(s) issued by a CA whose name the entry represents.

CRLs shall be stored in the LDAP Repository in the entry that appears in the CRL issuer name.

11.4 Object Class

When an LDAP repository is used:

- Entries that describe CAs shall be defined by organizationUnit structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes; and
- Entries that describe individuals (human entities) shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson. These entries shall also be a member of pkiUser auxiliary object class.

11.5 Attributes

When an LDAP repository is used:

- CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cPCPS attributes, as applicable; and
- User entries shall be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the PKI Repository.

12. ACRONYMS AND ABBREVIATIONS

CA	Certificate Authority
CARL	Certificate Authority Revocation List
CIMC	Certificate Issuing and Management Components
CMS	Card (Credential) Management System
COMSEC	Communications Security
CP	Certificate Policy
CPMA	Certificate Policy Management Authority
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FPKI OA	Federal Public Key Infrastructure Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E—X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
IDMS	Identity Management System
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union—Telecommunications Sector
ITU-TSS	International Telecommunications Union—Telecommunications System Sector
NIST	National Institute of Standards and Technology
NSA	National Security Entity
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

13. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NIST Computer Security Resource Center]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
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. [NIST Computer Security Resource Center]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an "applicant" after applying to the Certification Authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the Boeing PKI PA body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NIST Computer Security Resource Center, “audit”]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NIST Computer Security Resource Center, "audit trail"]
Audit Logs	The log of activity that is being performed by a user, system, or supporting procedural process based on assertions in this CPS.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NIST Computer Security Resource Center, “authentication”]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NIST Computer Security Resource Center, “backup”]
Binding	Process of associating two related elements of information. [NIST Computer Security Resource Center, “binding”]
Biometric	A physical or behavioral characteristic of a human being.
Card Management System (CMS)	A registration authority application responsible for issuance and maintenance of smartcard credentials.

Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. [ABADSG]. As used in this CP, the term “Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.
Certificate Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list of the certificates maintained by a CA which it has issued and that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NIST Computer Security Resource Center, “compromise”]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NIST Computer Security Resource Center, “confidentiality”]
Critical Certificates	Certificates issued to Root CAs and Issuing CAs, Enrollment Agent Certificates, Qualified Subordination Signing Certificate (QSS), Content Signer Certificates, and Key Recovery Agent Certificates.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NIST Computer Security Resource Center, “cryptoperiod”]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Entity as defined above.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End-entity	Relying Parties and Subscribers.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.

Boeing Operational Authority (Boeing OA)	The Boeing Public Key Infrastructure Operational Authority is the organization selected by the Boeing l Public Key Infrastructure Policy Authority to be responsible for operating the Boeing Certification Authority.
Boeing Public Key Infrastructure Policy Authority (PA)	The PA is a Boeing body responsible for setting, implementing, and administering policy decisions regarding interEntity PKI interoperability that uses the Boeing Principal CA or its Subordinate CAs.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NIST Computer Security Resource Center, “firewall”]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NIST Computer Security Resource Center, “integrity”]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA)	Agreement between the Boeing PA and any Entity allowing interoperability between the Boeing Principal CA and an Entity CA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Multi-Person	Refer to Two-Person Control
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NIST Computer Security Resource Center, “non-repudiation”] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.

PKI Component	Certification Authorities (CAs), Registration Authorities (RAs), Card Management Systems (CMSs), Certificate Status Authorities (CSAs), and in some references in this CP, it may include monitoring components and network components.
PKI Sponsor	“The Boeing Company” could be a sponsor for a human subscriber if an antecedent relationship were allowed (refer to 3.2.3.3). A “human subscriber” could be a “role” sponsor if issued a role certificate and allowed (refer to 3.2.3.4).
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the another Entity CA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
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.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.

Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Security Container	Safes, file cabinets, physical key management systems
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/subscriber. The RA/Trusted Agent controls the device utilized by the applicant/subscriber during the remote identity proofing process. The remote identity proofing process employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in section 5.3.3 of NIST SP 800-63A, dated June 2017; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.
System High	The highest security level supported by an information system. [NIST Computer Security Resource Center, “system high”]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NIST Computer Security Resource Center, “threat”]

Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trusted Workstation	Restricted workstations (also known as MyID, CMS/RA workstations, MAH Trusted Agent and Key Recovery workstations) used to access other PKI components.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NIST Computer Security Resource Center, “two-person control”]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401].

14. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FIPS 140	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html
NIST Glossary	NIST Computer Security Resource Center https://csrc.nist.gov/glossary
OCSP	Online Certificate Status Protocol
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.
RFC 4122	A Universally Unique Identifier (UUID) URN Namespace, Leach, Mealling, and Salz, July 2005 http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper et. al., May 2008 http://www.ietf.org/rfc/rfc5280.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Santesson, Myers et. al., June 2013 http://www.ietf.org/rfc/rfc6960.txt