

The Boeing Company
Boeing Commercial Airline PKI
Basic Assurance
CERTIFICATE POLICY

Version 1.1

PA Board Approved: March 11, 2011

Internal Tracking Doc No: G4650-ISS-PKI-233

Signature Page

John A. Lyons

Manager, Authentication Controls
Policy Authority Co-Chairperson

3-11-2011

Date

Kevin J. Murphy

Manager, Authentication Controls
Policy Authority Co-Chairperson

3-11-2011

Date

Approval of BCA PKI CP

by

BCA PKI Policy Authority

Method of Approval (Signature/Roll Call Vote)	Date of Approval	Version Number	CRs Applied
Roll Call Vote	02/02/2011	1.0	n/a
Roll Call Vote	03-11-11	1.1	CP_CR_03-11-11-01

Table of Contents

1 INTRODUCTION	13
1.1 OVERVIEW	13
1.2 DOCUMENT IDENTIFICATION.....	13
1.3 PKI PARTICIPANTS	13
1.3.1 PKI Authorities.....	13
1.3.2 Registration Authority (RA).....	14
1.3.3 End Entities	14
1.3.4 Relying Parties	14
1.3.5 Other Participants	15
1.3.6 Applicability	15
1.4 CERTIFICATE USAGE	15
1.4.1 Appropriate Certificate Uses	15
1.4.2 Prohibited Certificate Uses	15
1.5 POLICY ADMINISTRATION	16
1.5.1 Organization administering the document.....	16
1.5.2 Contact Person.....	16
1.5.3 Person Determining CP Suitability for the Policy	16
1.5.4 CP Approval Procedures	16
1.5.5 Waivers.....	16
2 Publication & Repository Responsibilities.....	17
2.1 PKI Repositories.....	17
2.1.1 Boeing Repository Obligations	17
2.2 Publication of Certificate Information.....	17
2.3 Time or Frequency Of Publication	17
2.4 Access Controls on PKI Repositories.....	17
3 Identification & Authentication.....	17
3.1 Naming	17
3.1.1 Types of Names.....	17

3.1.2	Need for Names to Be Meaningful.....	18
3.1.3	Anonymity or Pseudonymity of End Entities.....	18
3.1.4	Rules for Interpreting Various Name Forms	18
3.1.5	Uniqueness of Names	18
3.1.6	Recognition, Authentication, & Role of Trademarks	18
3.2	Initial Identity Validation	19
3.2.1	Method to Prove Possession of Private Key.....	19
3.2.2	Authentication of Organization Identity.....	19
3.2.3	Authentication of Individual Identity	19
3.2.4	Non-verified Subscriber Information	19
3.2.5	Validation of Authority	19
3.2.6	Criteria for Interoperation.....	19
3.3	Identification and Authentication For Re-Key Requests.....	19
3.3.1	Identification and Authentication for Routine Re-key	19
3.3.2	Identification and Authentication for Re-key after Revocation	20
3.4	Identification and Authentication For Revocation Request.....	20
4	Certificate Life-Cycle Operational requirements	20
4.1	Certificate Application	20
4.1.1	Submission of Certificate Application	20
4.1.2	Enrollment Process and Responsibilities.....	20
4.2	Certificate Application Processing.....	20
4.2.1	Performing Identification and Authentication Functions	21
4.2.2	Approval or Rejection of Certificate Applications.....	21
4.2.3	Time to Process Certificate Applications	21
4.3	Issuance	21
4.3.1	CA Actions during Certificate Issuance	21
4.3.2	Notification to Trusted Agent of Certificate Issuance.....	21
4.4	Certificate Acceptance.....	21
4.4.1	Conduct Constituting Certificate Acceptance	21
4.4.2	Publication of the Certificate by the CA	21
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	21

4.5 Key Pair and Certificate Usage	22
4.5.1 Subscriber Private Key and Certificate Usage	22
4.5.2 Relying Party Public Key and Certificate Usage.....	22
4.6 Certificate Renewal	22
4.7 Certificate Re-Key.....	22
4.8 Certificate Modification	22
4.9 Certificate Revocation & Suspension.....	23
4.9.1 Circumstances for Revocation of a Certificate.....	23
4.9.2 Who Can Request Revocation of a Certificate.....	23
4.9.3 Procedure for Revocation Request for End Entity Certificates	23
4.9.4 Revocation Request Grace Period	23
4.9.5 Time within which CA must Process the Revocation Request	23
4.9.6 Revocation Checking Requirements for Relying Parties	23
4.9.7 CRL Issuance Frequency.....	24
4.9.8 Maximum Latency of CRLs.....	24
4.9.9 On-line Revocation Availability.....	24
4.9.10 On-line Revocation Checking Requirements	24
4.9.11 Other Forms of Revocation Advertisements Available.....	24
4.9.12 Special Requirements Related To Key Compromise	24
4.9.13 Circumstances for Suspension.....	24
4.9.14 Who Can Request Suspension.....	24
4.9.15 Procedure for Suspension Request	24
4.9.16 Limits on Suspension Period.....	24
4.10 Certificate Status Services.....	24
4.11 End of Subscription	25
4.12 Key Escrow & Recovery	25
4.12.1 Key Escrow and Recovery Policy and Practices	25
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	25
5 Facility Management & Operations Controls.....	25
5.1 Physical Controls.....	25
5.1.1 Site Location & Construction.....	25

5.1.2 Physical Access	25
5.1.3 Power and Air Conditioning.....	25
5.1.4 Water Exposures.....	25
5.1.5 Fire Prevention and Protection	25
5.1.6 Media Storage.....	25
5.1.7 Waste Disposal	26
5.1.8 Off-Site backup	26
5.2 Procedural Controls	26
5.2.1 Trusted Roles.....	26
5.2.2 Number of Persons Required per Task.....	26
5.2.3 Identification and Authentication for Each Role.....	26
5.2.4 Roles Requiring Separation of Duties	26
5.3 Personnel Controls.....	27
5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements.....	27
5.3.2 Background Check Procedures.....	27
5.3.3 Training Requirements	27
5.3.4 Retraining Frequency and Requirements	27
5.3.5 Job Rotation Frequency and Sequence	27
5.3.6 Sanctions for Unauthorized Actions.....	27
5.3.7 Independent Contractor Requirements	28
5.3.8 Documentation Supplied To Personnel	28
5.4 Audit Logging Procedures.....	28
5.4.1 Types of Events Recorded.....	28
5.4.2 Frequency of Processing Log	28
5.4.3 Retention Period for Audit Logs	28
5.4.4 Protection of Audit Logs	28
5.4.5 Audit Log Backup Procedures.....	28
5.4.6 Audit Collection System.....	29
5.4.7 Notification to Event-Causing Subject.....	29
5.4.8 Vulnerability Assessments	29
5.5 Records Archive	29

5.5.1	Types of Records Archived	29
5.5.2	Retention Period for Archive.....	29
5.5.3	Protection of Archive	29
5.5.4	Archive Backup Procedures	29
5.5.5	Requirements for Time-Stamping of Records.....	29
5.5.6	Archive Collection System.....	29
5.5.7	Procedures to Obtain & Verify Archive Information.....	29
5.6	Key Changeover	29
5.7	Compromise & Disaster Recovery	30
5.7.1	Incident and Compromise Handling Procedures	30
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	30
5.7.3	Private Key Compromise Procedures.....	30
5.7.4	Business Continuity Capabilities after a Disaster.....	30
5.8	CA Termination.....	30
6	Technical Security Controls	31
6.1	Key Pair Generation & Installation	31
6.1.1	Key Pair Generation	31
6.1.2	Private Key Delivery to End Entity.....	31
6.1.3	Public Key Delivery to Certificate Issuer.....	31
6.1.4	CA Public Key Delivery to Relying Parties	31
6.1.5	Key Sizes	31
6.1.6	Public Key Parameters Generation and Quality Checking.....	32
6.1.7	Key Usage Purposes (as per X509 v3 key usage field).....	32
6.2	Private Key Protection & Cryptographic Module Engineering Controls.....	32
6.2.1	Cryptographic Module Standards & Controls	32
6.2.2	Private Key Multi-Person Control.....	32
6.2.3	Private Key Escrow	33
6.2.4	Private Key Backup.....	33
6.2.5	Private Key Archival.....	33
6.2.6	Private Key Transfer into or from a Cryptographic Module	33
6.2.7	Private Key Storage on Cryptographic Module	33

6.2.8 Method of Activating Private Keys	33
6.2.9 Methods of Deactivating Private Keys	33
6.2.10 Method of Destroying Private Keys	33
6.2.11 Cryptographic Module Rating	33
6.3 Other Aspects of Key Management.....	34
6.3.1 Public Key Archival	34
6.3.2 Certificate Operational Periods/Key Usage Periods.....	34
6.4 Activation Data.....	34
6.4.1 Activation Data Generation and Installation	34
6.4.2 Activation Data Protection	34
6.4.3 Other Aspects of Activation Data.....	34
6.5 Computer Security Controls	34
6.5.1 Specific Computer Security Technical Requirements	34
6.5.2 Computer Security Rating	35
6.6 Life-Cycle Security Controls.....	35
6.6.1 System Development and Configuration Controls	35
6.6.2 Security Management Controls	35
6.6.3 Life Cycle Security Ratings.....	35
6.7 NETWORK SECURITY CONTROLS.....	35
6.8 Time Stamping	35
7 Certificate, CARL/CRL, And OCSP profiles Format	36
7.1 Certificate Profile	36
7.1.1 Version Numbers.....	36
7.1.2 Certificate Extensions.....	36
7.1.3 Algorithm Object Identifiers	36
7.1.4 Name Forms	37
7.1.5 Name Constraints	37
7.1.6 Certificate Policy Object Identifier.....	37
7.1.7 Usage of Policy Constraints Extension	37
7.1.8 Policy Qualifiers Syntax & Semantics	37
7.1.9 Processing Semantics for the Critical Certificate Policy Extension.....	37

7.2 CRL Profile	37
7.2.1 Version Numbers.....	37
7.2.2 CRL and CRL Entry Extensions	38
7.3 OCSP Profile	38
8 Compliance Audit & Other Assessments	38
8.1 FREQUENCY OF AUDIT OR ASSESSMENTS	38
8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR	38
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	38
8.4 TOPICS COVERED BY ASSESSMENT	38
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY	38
8.6 Communication of Results	38
9 Other Business & Legal Matters	39
9.1 FEES.....	39
9.2 FINANCIAL RESPONSIBILITY.....	39
9.2.1 Insurance Coverage	39
9.2.2 Other Assets	39
9.2.3 Insurance/warranty Coverage for End-Entities	39
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION	39
9.3.1 Scope of Confidential Information	39
9.3.2 Information not within the scope of Confidential Information	39
9.3.3 Responsibility to Protect Confidential Information.....	40
9.4 PRIVACY OF PERSONAL INFORMATION.....	40
9.4.1 Privacy Plan.....	40
9.4.2 Information treated as Private	40
9.4.3 Information not deemed Private	40
9.4.4 Responsibility to Protect Private Information	40
9.4.5 Notice and Consent to use Private Information.....	40
9.4.6 Disclosure Pursuant to Judicial/Administrative Process	40
9.4.7 Other Information Disclosure Circumstances	40
9.5 INTELLECTUAL PROPERTY RIGHTS.....	41
9.5.1 Property Rights in Certificates and Revocation Information	41

9.5.2 Property Rights in the CP	41
9.5.3 Property Rights in Names.....	41
9.5.4 Property Rights in Keys and Key Material.....	41
9.6 REPRESENTATIONS & WARRANTIES	41
9.6.1 Subject to Section 9.17.1 (Order of Precedence), CA Representations and Warranties.....	41
9.6.2 RA Representations and Warranties.....	42
9.6.3 End Entities Representations and Warranties.....	42
9.6.4 Relying Parties Representations and Warranties.....	42
9.6.5 Representations and Warranties of other Participants.....	42
9.7 DISCLAIMERS OF WARRANTIES	42
9.8 LIMITATIONS OF LIABILITY	42
9.9 INDEMNITIES	43
9.9.1 Indemnification by End Entities.....	43
9.9.2 Indemnification by Relying Parties	43
9.10 TERM & TERMINATION	43
9.10.1 Term	43
9.10.2 Termination	43
9.10.3 Effect of Termination and Survival	43
9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS.....	43
9.12 AMENDMENTS.....	43
9.12.1 Procedure for Amendment	43
9.12.2 Notification Mechanism and Period.....	44
9.12.3 Circumstances under which OID must be changed.....	44
9.13 DISPUTE RESOLUTION PROVISIONS	44
9.13.1 Disputes among Boeing, Affiliates, and Customers.....	44
9.13.2 Disputes with End-User Subscribers or Relying Parties	44
9.14 GOVERNING LAW	44
9.15 COMPLIANCE WITH APPLICABLE LAW	45
9.16 MISCELLANEOUS PROVISIONS	45
9.16.1 Entire agreement.....	45
9.16.2 Assignment.....	45

9.16.3 Severability.....	45
9.16.4 Enforcement (Attorney Fees/Waiver of Rights).....	45
9.16.5 Force Majeure.....	45
9.17 OTHER PROVISIONS 9.17.1 Order of Precedence.	45
10 Certificate, CRL, and OCSP Formats.....	45
10.1 Boeing Commercial Airline PKI Airline Private Certificate Authority Signing Certificate	45
10.2 Airplane Identity Certificate.....	47
10.3 Maintenance Laptop Identity Certificates	49
10.4 Application Identity (SSL) Certificates	51
10.5 LSAP Librarian Suite Object Signing Certificates.....	53
10.6 Airline Trusted Agent Identity Certificates	55
10.7 Full and Complete CRL.....	56
11 PKI Repository Interoperability Profile	57
11.1 Protocol	57
11.2 Authentication	57
11.3 Naming	57
11.4 Object Class.....	57
11.5 Attributes	57
12 ACRONYMS & ABBREVIATIONS	57
13 GLOSSARY	58
14 BIBLIOGRAPHY	65
15 ACKNOWLEDGEMENTS	66

1 INTRODUCTION

1.1 OVERVIEW

This Certificate Policy (CP) is a governance document that defines issuance policies for certificates issued by The Boeing Company (Boeing) to support Airline customers that have contracted with Boeing to deploy and operate an e-Enabled Ground System (EGS) on their behalf. The CP is not a legal agreement between Boeing and any participant in Boeing Commercial Airline PKI (BCA PKI); rather, contractual obligations between Boeing and all other parties are established by means of separate written agreements between the parties.

Certificates in this environment are issued at the Basic level of assurance. The Basic level of assurance as defined by the United States Government Federal Bridge Certificate Policy as approved by the Federal PKI Policy Authority is relevant “to environments where there are risks and consequences of data compromise but are not considered to be of major significance”. The word “assurance” in this CP means a Relying Party can be reasonably assured of the identity binding to the public key.

The Relying Party may distinguish the assurance level of the certificate by the OID value in the certificate policy extension.

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.2 DOCUMENT IDENTIFICATION

The Boeing Certificate Policy document is assigned a Boeing Object Identifier number. Boeing has a Private Enterprise OID number, assigned and registered by the Internet Assigned Numbers Authority (IANA) <http://www.iana.org>.

The Boeing OID arc for this Commercial Airline PKI Certificate Policy document is:
1.3.6.1.4.1.73.15.3.1.6

1.3 PKI PARTICIPANTS

1.3.1 PKI Authorities

1.3.1.1. Boeing Commercial Airline PKI Policy Authority (PA)

The Boeing Commercial Airline PKI Policy Authority (BCA PKI PA) is a group of individuals responsible for the direction and operation of the Boeing Commercial Airline PKI. The PA facilitates:

- Approval of the Boeing Commercial Airline PKI CP
- Review and approval for major operational changes

- Approval for architecture changes
- Incident management review
- Approval of trust relationships

1.3.1.2 Boeing Operational Authority

The Boeing operational authority (OA) is the organization that operates the CAs, including issuing CA certificates, posting those certificates and Certification Authority Revocation Lists (CRLs) into the repository, and facilitating the continued availability of the repository to all relying parties.

1.3.1.3 Airline e-Enabling Support Certificate Authority (CA)

The Airline e-Enabling Support Certificate Authority is a self-signed CA authorized to create and issue Airline Trusted Agent Identity Certificates, Airplane Identity Certificates, Application Identity Certificates, Maintenance Laptop Identity Certificates and LSAP Librarian Suite object signing Certificates.

1.3.2 Registration Authority (RA)

The Registration Authority function within the Boeing Commercial Airline PKI environment is performed by the CAS Trusted Agent role.

1.3.3 End Entities

An end entity is the entity whose name, e-mail or other unique identification number appears as the subject in a certificate and who asserts that it uses its key and certificate in accordance with this policy. The targeted Boeing Commercial Airline end entities include but are not limited to the following categories of entities that may wish to communicate securely.

- Human Subscribers – Boeing employees fulfilling the Trusted Agent role.
- Non-Human End Entities – airplanes, applications, servers, maintenance laptops and the LSAP Librarian Suite.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the end entity's identity to a public key. The Relying Party is solely responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as CP identifiers or key usages) to determine in its sole discretion the suitability of the certificate for a particular use. Boeing accepts no responsibility for Relying Parties' use of certificates and any information therein. Relying Parties shall not use certificates and any information therein in connection with a Prohibited Certificate Use (see section 1.4.2)

1.3.5 Other Participants

The CAs operating under this CP may require the services of other Boeing operational, administrative, security and application authorities.

1.3.6 Applicability

Entities must independently evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information or resources being accessed. This evaluation is done solely by each Relying Party for each application and is not controlled by this CP or by Boeing.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must independently evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done independently by each organization for each application and is not controlled by this CP or by Boeing.

Specific cryptographic function permitted using the certificate and its corresponding keys, such as:

Server Authentication, SSL Session Key Encipherment, Client Authentication, Digital Signature or CodeSigning

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular be used only to the extent permitted by applicable export or import laws.

Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Basic Assurance Certificates shall not be used as proof of identity or as support of non repudiation of identity or authority. Application Certificates are intended for applications and shall not be used as server or organizational Certificates.

CA Certificates must not be used for any functions except CA functions. In addition, end entity Certificates must not be used as CA Certificates.

Prohibited Certificate Uses include, but are not limited to, the following applications:

- Any export, import, use or activity that contravenes any local or international laws or regulations

- Any usage of certificates in conjunction with illegal activities
- Any usage of certificates for personal use or purposes not related to company business
- Any use of a certificate after it has been suspended or revoked
- Any usage inconsistent with the key usage and basic constraints specified in the certificate profiles
- Any usage not supported by a contractual relationship between Boeing, customer airlines, and/or other parties involved in supporting airline operations as specifically authorized by the airline customer

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

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

1.5.2 Contact Person

The Boeing Company
Attn: BCA PKI Policy Authority Chair
Mail Code: 7L-07
PO BOX 3707
SEATTLE WA 98124-2207
UNITED STATES

1.5.3 Person Determining CP Suitability for the Policy

The BCA PKI Policy Authority determines the suitability and applicability of this CP.

1.5.4 CP Approval Procedures

Approval of this CP and subsequent amendments are made by the Boeing Commercial Airline PKI Policy Authority. Amendments are in the form of a document containing an amended form of the CP. Updates supersede any designated or conflicting provisions of any previous version of the CP. The Boeing Commercial Airline PKI Policy Authority may determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Certificate.

1.5.5 Waivers

The Boeing Commercial Airline PKI Policy Authority does not issue waivers to CAs asserting compliance to this policy.

2 Publication & Repository Responsibilities

2.1 PKI REPOSITORIES

The Boeing Operational Authority has taken reasonable steps to utilize repositories to support Boeing Commercial Airlines PKI operations. Repositories are used to hold information that may be required by end entities or relying parties and may contain information such as:

- Certificates and public key information
- Revocation status and CRL files

2.1.1 Boeing Repository Obligations

The Boeing Operational Authority uses a publicly accessible online repository for posting and retrieval stipulations of this CP.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

Boeing maintains a web-based repository that permits relying parties to make online inquiries regarding revocation and other certificate status information. A copy of this Policy and the CRL is publicly available on the Boeing public repository website (see <http://crl.boeing.com/crl/>)

2.3 TIME OR FREQUENCY OF PUBLICATION

The CRL is published as outlined in this CP. All information to be published in the repository is published in a reasonable timeframe after such information becomes available to the CA.

2.4 ACCESS CONTROLS ON PKI REPOSITORIES

Information in the Boeing public PKI repositories is accessible for reading from the Internet. This information may be obtained without authentication.

3 Identification & Authentication

3.1 NAMING

Unless where indicated otherwise in this CP, the digital certificate names appearing in issued certificates are authenticated.

3.1.1 Types of Names

Subscriber Certificates contain an X.500 distinguished name in the Subject name field. Specific formats are outlined in the certificate profiles. Subject names are expected to identify unique Airline entities, but these entities are not tracked within the Boeing Commercial Airline PKI or directories.

The CAS Trusted Agent will take reasonable steps to confirm that Subject names with all certificate requests are appropriate to the Airline customer requirements, and that all CSR contents adhere to requirements specified in this policy including:

Providing Boeing with express permission to issue certificates to identities in the Airline customer namespace, including, but not limited to:

- the Organization (O=) component in every certificate shall be the legal name of the customer Airline organization,
- if Common Name (CN=) components in a certificate contain a fully qualified DNS domain name, the Airline customer shall have all legal right, title and interest in and to the domain name.

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 should identify in a meaningful way the end entity to which they are assigned.

3.1.3 Anonymity or Pseudonymity of End Entities

The Airline e-Enabling Support CA shall take reasonable steps to prevent the issuance of anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable Certificate Profile found in section 10 of this CP.

3.1.5 Uniqueness of Names

Subject names will be in the namespace of the Airline customer, and thus name uniqueness will only be checked by the Airline and Boeing Trusted Agents.

End-entity distinguished names should be unique, and a Unique Identifier attribute may be specified. It is acceptable for multiple certificates to be issued to the same Subject.

3.1.6 Recognition, Authentication, & Role of Trademarks

Airlines shall not use names in their certificate requests that infringe upon the Intellectual Property Rights of others. Boeing is not required to determine whether an airline has Intellectual Property Rights in the name appearing in a certificate requests or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and Boeing shall be entitled, without liability to any airline, to reject or suspend any certificate requests because of such dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where an entity named in a certificate generates its own keys, that entity is 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 entity's public key.

3.2.2 Authentication of Organization Identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by the CAS Trusted Agent is confirmed in accordance with procedures set forth in the Boeing Commercial Airline Environment.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

Boeing CAS Trusted Agents receive credentials as part of the vetting process by the CA Administrator.

3.2.3.2 Non-Human End Entity Certificates

Non-human end-entity certificates must be sponsored by a Boeing CAS Trusted Agent. The TA is responsible for providing a valid CSR to the CA. The registration information must be verified to an assurance level commensurate with the certificate assurance level being requested.

3.2.4 Non-verified Subscriber Information

Subject name Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Whenever an end entity name is associated with an organization name in a certificate in such a way to indicate the end entity affiliation or authorization to act on behalf of the organization the CAS TA is responsible for verifying airline affiliation.

3.2.6 Criteria for Interoperation

Not Applicable

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old certificate is being replaced with a new certificate and not emphasizing whether or not a new key pair is

generated. This distinction is not important as a new key pair is always generated as part of the Boeing Commercial Airline PKI end-entity certificate replacement process.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked the end entity is required to go through the initial registration process to obtain a new certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation procedures are designed to confirm that, prior to any revocation of any certificate, the revocation has in fact been requested by the CAS Trusted Agent. The CAS Trusted Agents are entitled to request the revocation of end-entity certificates within the CA's domain.

4 Certificate Life-Cycle Operational requirements

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Application

The following may submit certificate applications:

- CAS Trusted Agents for non-human end entity certificates
- OA Organization for CA and CAS Trusted Agent certificates

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End Entity Certificates

CAS Trusted Agent certificates can only be issued by the OA Organization after the CAS Trusted Agent has completed the vetting process. Non-human end entity certificates can only be requested by the CAS Trusted Agent.

4.1.2.2 CA Certificates

The Boeing Commercial Airline PKI may issue a new CA certificate for this environment only upon execution of a separate written contract and only with approval from the Boeing Commercial Airlines PKI Policy Authority.

4.2 CERTIFICATE APPLICATION PROCESSING

The CA and CAS Trusted Agent will take reasonable steps to verify that the information in certificate applications is accurate.

4.2.1 Performing Identification and Authentication Functions

The Airline e-Enabling Support CA will take reasonable steps to identify and authenticate the CAS Trusted Agent.

4.2.2 Approval or Rejection of Certificate Applications

The certificate may only be approved if the identity verification procedures for the CAS Trusted Agent have been successfully completed.

4.2.3 Time to Process Certificate Applications

CAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing, unless otherwise indicated in a separate written agreement.

4.3 ISSUANCE

4.3.1 CA Actions during Certificate Issuance

A certificate is created and issued following the approval of a certificate request by a CAS Trusted Agent. The CA creates and issues non-human end entity certificates to the CAS Trusted Agent for distribution to end entities.

A CAS Trusted Agent certificate is created and issued following the approval by the Operational Authority.

4.3.2 Notification to Trusted Agent of Certificate Issuance

End Entity certificates shall be made available to CAS Trusted Agents by allowing them to download from the CA.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

For self-signed CAs, there is no formal acceptance of self-signed CA certificates. For end-entity certificates, the CAS Trusted Agent taking possession of the certificate constitutes as acceptance.

4.4.2 Publication of the Certificate by the CA

The Boeing Commercial Airline PKI does not publish the end entity certificates it issues.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

For the Airline eEnabling Support CA, the Boeing OA notifies CAS Trusted Agents of new certificates issued. Notification of end-entity certificate issuance is not required.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

End Entities shall protect their private keys from access by unauthorized 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

The certificates specify restrictions on use through certificate extensions, including the basic constraints, certificate policies, and key usage extensions. The Airline eEnabling Support CAs issue Certificate Revocation Lists (CRL) which contain a list of serial numbers of all revoked, but not expired, certificates. Relying Parties shall process and comply with the information in the certificates and CRL whenever using Boeing-issued certificates. This includes full certificate validation, CA chain validation, revocation checking, and honoring critical extensions [reference IETF RFC 5280]

Relying parties must use public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates. Relying Parties shall not use public keys in connection with any Prohibited Certificate Use in section 1.4.2.

4.6 CERTIFICATE RENEWAL

The Boeing Commercial Airline PKI policy does not permit certificate renewals. If a certificate is nearing expiration, new keys and a new certificate request must be generated in order to replace the certificate.

4.7 CERTIFICATE RE-KEY

Generally speaking, both “Rekey” and “Renewal” are commonly described as “Certificate Renewal”, focusing on the fact that the old certificate is being replaced with a new certificate and not emphasizing whether or not a new key pair is generated. This distinction is not important as a new key pair is always generated as part of the Boeing Commercial Airline PKI end-entity certificate replacement process.

4.8 CERTIFICATE MODIFICATION

The Airline eEnabling Support CA does not permit certificate modifications. If information in a certificate needs to be modified, the end entity, or CA using the certificate must enroll for a new certificate.

4.9 CERTIFICATE REVOCATION & SUSPENSION

4.9.1 Circumstances for Revocation of a Certificate

Only in the circumstances listed below, will an Airline e-Enabling Support CA certificate be revoked by the OA and published on a CRL.

- The first circumstance is when the Operational Authority receives an authenticated request from CAS designated officials of the PKI who may request a certificate to be revoked.
- The second circumstance is when the Boeing operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by Boeing.

An end entity certificate may be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid.

Revoked certificates are placed on the CRL. Revoked certificates are included on all new publications of the CRL until the certificates expire.

4.9.2 Who Can Request Revocation of a Certificate

Under the two circumstances listed above for revocation of CA Certificates the Policy Authority Chair may authorize immediate CA certificate revocation. The Policy Authority will meet as soon as practical to review the emergency revocation.

The Operational Authority can approve revocation of the CAS Trusted Agent certificate. Non-human end entity certificates can be requested for revocation by the CAS Trusted Agent.

4.9.3 Procedure for Revocation Request for End Entity Certificates

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.

4.9.4 Revocation Request Grace Period

For Boeing CAs operating under this policy, revocation request processing time shall be as soon as practical.

4.9.5 Time within which CA must Process the Revocation Request

Commercially reasonable steps are taken to process revocation requests.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates is prohibited. The matter of how often new revocation data should be obtained is a determination to be made solely by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed. Boeing accepts no responsibility for Relying Parties' use of certificates and any information therein.

4.9.7 CRL Issuance Frequency

Boeing will issue CRL files for end entities approximately every three days. In the case of operational failure, the current CRL may be resigned and reissued before the expiration of the validity period.

A special long-lived CRL file is also created, for provisioning onto the Airplane. This CRL is re-issued annually or more frequently as needed due to certificate revocations.

4.9.8 Maximum Latency of CRLs

No stipulation.

4.9.9 On-line Revocation Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

Special CRLs for provisioning onto Airplanes are only available on the CA's web interface and only accessible by authenticated CAS Trusted Agents.

4.9.12 Special Requirements Related To Key Compromise

No stipulation beyond what is already covered by this CP

4.9.13 Circumstances for Suspension

The Boeing Commercial Airline Certificate Policy does not permit 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 do not use certificate status services such as SCVP or OCSP.

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW & RECOVERY

Key escrow is not permitted as part of this Boeing Commercial Airline PKI.

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable

5 Facility Management & Operations Controls

5.1 PHYSICAL CONTROLS

5.1.1 Site Location & Construction

All CA operations are conducted within a physically protected environment that is designed to increase the CA's ability to deter, prevent and detect unauthorized use of, access to or disclosure of sensitive information and systems.

5.1.2 Physical Access

CAs are accessible by means of commercially acceptable multi-level physical controls.

5.1.3 Power and Air Conditioning

The CA will be run in commercially acceptable data centers with contingencies for backup power.

5.1.4 Water Exposures

No stipulation

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

Media is stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic).

5.1.7 Waste Disposal

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

5.1.8 Off-Site backup

CAs maintain back ups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted roles may perform functions that introduce security issues if not carried out properly, whether accidentally or maliciously. The functions performed in these roles form the basis of trust for the PKI.

Trusted Persons include, but are not limited to:

- CA Administrators
- IT Administrators
- Internal Auditors
- CAS Trusted Agents
- Trusted Agent Workstation Administrator

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:

- CA Key generation
- CA private key backup

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

5.2.3 Identification and Authentication for Each Role

An individual will reasonably identify and authenticate him/herself before being permitted to perform any actions for that role.

5.2.4 Roles Requiring Separation of Duties

Separation of duties means the trusted person filling a role cannot complete the duties of another trusted role. Roles requiring separation of duties include (but are not limited to):

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation

- requests, key recovery requests or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

Personnel in trusted roles are vetted thoroughly by the OA office through means that may include DoD security clearances or other means.

5.3.2 Background Check Procedures

Boeing personnel in trusted roles may receive background checks prior to role appointment.

5.3.3 Training Requirements

The OA takes reasonable steps to ensure personnel performing duties with respect to the operation of the CA receive training, including training in the following areas:

- CA security principles and mechanisms
- PKI software versions in use on the CA systems
- PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy

5.3.4 Retraining Frequency and Requirements

CAs may provide refresher training and updates to personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Boeing may establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the PKI may be subject to the same criteria as Boeing employees.

5.3.8 Documentation Supplied To Personnel

Reasonable documentation sufficient to define duties and procedures for each role may be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

Audit log files may be generated for all events relating to the security of the CA. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. The security audit logs for each event defined in this section are maintained in accordance with this CP.

5.4.1 Types of Events Recorded

The types of auditable events that are recorded by CAs are set forth below. Logs, whether electronic or manual, contain the date and time of the event, and the identity of the entity that caused the event. Types of auditable events may include:

- Operational events
- Certificate lifecycle events
- Trusted role actions
- Discrepancy and compromise reports

5.4.2 Frequency of Processing Log

Audit logs are reviewed in response to alerts based on irregularities and incidents within the CA system.

5.4.3 Retention Period for Audit Logs

Retention period for audit logs are retained onsite for a reasonable period of time designated by Boeing operations.

5.4.4 Protection of Audit Logs

Audit logs may be protected with mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries may be backed up, and copies may be archived annually.

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited.

5.4.8 Vulnerability Assessments

The OA may take reasonable steps to perform routine self-assessments of security controls.

5.5 RECORDS ARCHIVE

5.5.1 Types of Records Archived

CA archive records may be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate issued by the CA.

5.5.2 Retention Period for Archive

The archive records may be retained for the life of the end entity certificates.

5.5.3 Protection of Archive

No unauthorized person is permitted to write to, modify or delete the archive.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information need not be cryptographically based.

5.5.6 Archive Collection System

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain & Verify Archive Information

Only members of the Operational Authority are able to obtain authorized access to the archive.

5.6 KEY CHANGEOVER

A CA Certificate may be re-issued if ordered by the Boeing Commercial Airlines PKI Policy Authority.

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Backups of CA information shall be kept in off-site storage and made available in the event of a compromise or disaster.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If the CA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the CA will take reasonable steps to promptly reestablished operation, subject to the ability to generate certificate status information. The Boeing Commercial Airlines PKI PA and CAS shall be notified as soon as possible.

If the CA signature keys are destroyed, the CA will take reasonable steps to promptly reestablish operations, subject 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 notified immediately. This will assist other CAs in protecting their end entity interests as Relying Parties. If revocation capability cannot be established in a reasonable time-frame, the CA may determine whether to request revocation of its certificate(s).

5.7.3 Private Key Compromise Procedures

In the event of a CA private key compromise that CA will be revoked, and the Boeing OA will notify the Boeing Commercial Airline PKI Policy Authority Board.

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 BCA PKI PA and Boeing Commercial Airplane Services shall be notified at the earliest feasible time, and the PA shall direct the OA to revoke or recover the CA certificates, and direct the CA to follow the appropriate procedures outlined in this CP. Relying parties may decide in their sole discretion whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificate. Boeing accepts no responsibility for such use by Relying Parties.

5.8 CA TERMINATION

In the event of termination of the Airline e-Enabling Support CA operation, certificates signed by the Airline e-Enabling Support CA will be revoked and the Boeing Commercial Airline PKI Policy Authority will advise Boeing Commercial Airplane Services (CAS) that the CA operation has been terminated.

6 Technical Security Controls

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation

Random numbers for keys and keys used to sign certificates, CRLs or status information by any Boeing CA will be generated in FIPS 140-2 level 2 validated hardware cryptographic modules or modules validated under equivalent international standards.

Multiparty control is required for CA key pair generation for the CAs operating under this policy.

6.1.2 Private Key Delivery to End Entity

The CAs generate their own key pair and therefore do not need private key delivery.

If an end entity generates their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs generate keys on behalf of the non-human end entity, then the private key shall be delivered securely to the CAS Trusted Agent. In all cases, the following requirements shall be met:

- Anyone who generates a private signing key for an end entity shall not retain any copy of the key after delivery of the private key to the end entity
- The private key shall be protected from activation, compromise, or modification during the delivery process.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the CAS Trusted Agent, the public key and the End Entity's identity shall be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the End Entity's verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of the Airline e-Enabling Support CA signing certificate will be provided to the end entities acting as relying parties in a secure manner so that the CA certificate is not vulnerable to modification or substitution.

6.1.5 Key Sizes

If the Boeing Commercial Airline PKI Policy Authority determines that the security of a particular algorithm may be compromised, it may require the CAs to revoke the affected certificates. All certificates and Transport Layer Security (TLS) protocols shall use the following algorithm suites.

Cryptographic Function	2048 Bit
Signature	2048 bit RSA per FIPS 186- For ECDSA, per FIPS 186-2, 224 bit prime field or 233 bit binary field
Hashing	SHA-1 or higher
Public Key Encryption	2048 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 224 bit prime field or 233 bit binary field
Symmetric Encryption	3 Key TDES or AES

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Key Usage Purposes (as per X509 v3 key usage field)

The use of a specific key is determined by the key usage extension in the X.509 certificate found in the certificate profile.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Boeing has implemented a combination of physical, logical, and procedural controls to increase the security of Boeing and Airline e-Enabling Support CA private keys. End Entities shall take all necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys. Boeing accepts no responsibility for the security of End Entities' private keys.

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. The Boeing Commercial Airline PKI Policy Authority may determine that other comparable validation, certification, or verification standards are sufficient.

6.2.2 Private Key Multi-Person Control

A single person shall not be permitted to invoke the complete CA signature or access any cryptomodule containing the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control.

6.2.3 Private Key Escrow

Private Keys will not be escrowed in the Boeing Commercial Airline PKI.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

All CA private signature keys will only be maintained on disk and backed up in encrypted form.

6.2.4.2 Backup of End Entity Private Signature Key

End Entity private signature keys whose corresponding public key is contained in a certificate may be backed up or copied for backup purposes, but this back up copy must be retained only in the end-entity's control.

6.2.5 Private Key Archival

Private Keys shall not be archived by the CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA's private keys that are generated in a cryptographic module must remain only in the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Keys

All participants in the Boeing Commercial Airline Environment shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9 Methods of Deactivating Private Keys

For online certificate authorities: the activated Cryptographic modules will be left unattended but with commercially acceptable methods to ensure the CA is reasonably secured.

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.

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 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.

Key	Recommended Validity Period
Airline CA	20 years
Airline Airplane Identity	3 Year
Airline Maint Laptop Identity	1 Year
Airline LSAPL Suite Object Signing	3 Years
Airline SSL Application Identity	3 Year
Airline Trusted Agent	3 Year

Boeing does not guarantee the sufficiency of any recommended validity period.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and meet the applicable security policy requirements used to store the keys.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Commercially reasonable computer security functions are provided by the operating system or through a combination of operating system, software, and physical safeguards.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development and Configuration Controls

Boeing uses software for CA functions that is developed within a systems development environment that meets commercially acceptable practices:

- Software is developed in a controlled environment. This requirement does not apply to commercial off-the-shelf hardware or software.
- The hardware and software is 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.
- Care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations are obtained from sources authorized by local policy. CA hardware and software are scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates are purchased or developed in the same manner as original equipment and installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades are documented and controlled. Mechanisms are established to facilitate detection of unauthorized modification to the CA software or configuration.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

CA functions are performed using networks that are secured in accordance with industry standards in order to deter unauthorized access, tampering, and denial-of-service attacks.

6.8 TIME STAMPING

Certificates, CRLs, and other revocation database entries may contain time and date information. Such time information need not be cryptographic-based.

7 Certificate, CARL/CRL, And OCSP profiles Format

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure yet be flexible enough to meet the needs of the various CAs and communities. PKIs issuing certificates asserting this CP shall comply with RFC 5280. Critical private extensions shall be interoperable in their intended community of use. Issuer CA and End Entity certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP. Section 10 contains the certificate formats.

7.1.3 Algorithm Object Identifiers

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

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha1	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA1(1)}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-Specified(3) ecdsa-with-Sha256 (2)}

Certificates under this CP use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

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 base certificate shall be populated with a unique X.500 Distinguished Name, with the attribute types as further constrained by RFC 5280. DNs shall be encoded as printable strings if possible. If that is not possible, the only acceptable alternative is UTF8. In all cases the CA DN and name space for name constraints shall be encoded as a printable string.

7.1.5 Name Constraints

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

The Issuer CA may obscure an End Entity Subject name to meet local privacy regulations as long as such name is unique and traceable to a corresponding unobscured name. Issuer names may not be obscured. Issuer CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to each certificate is set forth in Section 1.2. The Certificate Policies extension in each certificate is populated in accordance with Section 1.2.

7.1.7 Usage of Policy Constraints Extension

The Boeing CAs adhere to the Certificate Formats described in this CP.

7.1.8 Policy Qualifiers Syntax & Semantics

Certificates issued under this CP shall not contain policy qualifiers

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by the CA conforms to X.509 certification path processing rules.

7.2 CRL PROFILE

7.2.1 Version Numbers

The CAs issue either X.509 Version one (1) or two (2) CRLs. Populate version 1 with (0) integer and version 2 with (1) integer.

7.2.2 CRL and CRL Entry Extensions

The CRL and CRL entry extensions comply with the CRL profile specified in section 10.

7.3 OCSP PROFILE

Not applicable

8 Compliance Audit & Other Assessments

The Boeing Operational Authority may take reasonable steps to implement compliance audit mechanisms to confirm that the requirements of applicable CP are being implemented and enforced.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

Airline e-Enabling Support CAs may be subject to internal audit periodically to validate operations are occurring in accordance with the CP.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The internal audit function is a role separated function that may be performed by an individual who has no other trusted role within the Boeing Commercial Airline PKI.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The auditor shall not be part of the Boeing Operational Authority.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of the audit is to verify that operation of the CA complies with the requirements of this CP.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, the following actions shall be performed:

- The compliance auditor notes the discrepancy;
- The compliance auditor then notifies the Operational Authority;

8.6 COMMUNICATION OF RESULTS

Audit results will be communicated to the Operational Authority. The OA will determine if the PA needs to be informed. Audit results will not be made available outside Boeing.

9 Other Business & Legal Matters

9.1 FEES

No stipulation outside applicable contractual agreements.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Customers and End Entities (each a “Customer” for this purposes of this Article 9) are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other Assets

Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance/warranty Coverage for End-Entities

No Stipulation

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The following, subject to Section 9.3.2, be kept confidential and private (“Confidential/Private Information”):

- Certificate request records,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Boeing,
- Audit reports created by Boeing
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of Boeing hardware and software and the administration of certificate services and designated enrollment services.

9.3.2 Information not within the scope of Confidential Information

Certificates, certificate revocation and other status information, Boeing repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Boeing provides reasonable security for confidential information to protect from compromise and disclosure to third parties.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

No Stipulation

9.4.2 Information treated as Private

Any information about End Entities that is not publicly available through the content of the issued certificate and online CRLs is treated as private.

9.4.3 Information not deemed Private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

Boeing Commercial Airline PKI personnel receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to use Private Information

Unless where otherwise stated in this CP, or by separate written agreement, private information will not be used without the consent of the party to whom that information applies.

This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Boeing shall be entitled to disclose Confidential/Private Information if, in good faith, Boeing believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 INTELLECTUAL PROPERTY RIGHTS

The allocation of Intellectual Property Rights among Boeing Commercial Airline PKI participants other than Relying Parties is governed by the applicable agreements among such Boeing Commercial Airline PKI participants. Subject to Section 9.17.1 (Order of Precedence), the following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

Boeing retains all Intellectual Property Rights in and to the certificates and revocation information that they issue subject to Section 9.17.1 (Order of Precedence).

Customer's right to reproduce and distribute certificates is as provided by way of a separate Boeing-Customer agreement. Customers grant permission to reproduce and distribute certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of certificates is subject to any other applicable agreement referenced in the certificate, if any. Subject to Section 9.17.1 (Order of Precedence), Customers shall grant permission to use revocation information to perform Relying Party functions subject to or any other applicable agreements.

9.5.2 Property Rights in the CP

Participants acknowledge that Boeing retains all Intellectual Property Rights in and to this CP.

9.5.3 Property Rights in Names

A Customer retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any certificate issued to such Customer.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to certificates of CAs and end-entity are the property of the CAs and End Entities that are the respective Subjects of these certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, Boeing's CA public keys and the certificates containing them, including all Airline e-Enabling Support CA self-signed certificates, are the property of Boeing.

9.6 REPRESENTATIONS & WARRANTIES

9.6.1 Subject to Section 9.17.1 (Order of Precedence), CA Representations and Warranties

CAs warrant that:

- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the Certificate Application or issuing the certificate,

- There are no errors in the information in the certificate that were introduced by the entities approving the Certificate Application or issuing the certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the certificate,
- Their certificates meet all material requirements of this CP, and
- Revocation services and use of a repository conform to the applicable CP in all material aspects.
- Subject to Section 9.17.1 (Order of Precedence), Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

No stipulation outside applicable contractual agreements.

9.6.3 End Entities Representations and Warranties

No stipulation outside applicable contractual agreements.

9.6.4 Relying Parties Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of other Participants

No stipulation outside applicable contractual agreements.

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, Boeing disclaims all warranties with respect to certificates, including but not limited to, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS; ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE; ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING; AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OF OR DAMAGE TO ANY AIRCRAFT.9.8 LIMITATIONS OF LIABILITY.

9.8 LIMITATIONS OF LIABILITY

BOEING WILL HAVE NO OBLIGATION OR LIABILITY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING) OR OTHERWISE, FOR LOSS OF USE, REVENUE OR PROFIT OR FOR ANY OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN ANY CERTIFICATE.

9.9 INDEMNITIES

9.9.1 Indemnification by End Entities

No stipulation outside applicable contractual agreements.

9.9.2 Indemnification by Relying Parties

No stipulation

9.10 TERM & TERMINATION

9.10.1 Term

The CP becomes effective upon publication in the Boeing repository. Amendments to this CP become effective upon publication in the Boeing repository.

9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, Boeing Commercial Airline PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

Unless otherwise specified by agreement between the parties, Boeing Commercial Airline PKI participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Amendments to this CP may be made by the Boeing Commercial Airline PKI Policy Authority. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The PA shall determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate policies.

9.12.2 Notification Mechanism and Period

The Boeing Commercial Airline PKI Policy Authority reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PA's decision to designate amendments as material or non-material shall be within the Boeing Commercial Airline PKI Policy Authority's sole discretion.

Notwithstanding anything in the CP to the contrary, if the Policy Authority believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of its system or any portion of it, Boeing and the Policy Authority shall be entitled to make such amendments by publication in the Boeing Repository. Such amendments will be effective immediately upon publication.

9.12.3 Circumstances under which OID must be changed

If the OA determines that a change is necessary in the object identifier corresponding to a certificate policy, the amendment shall contain new object identifiers for the certificate policies corresponding to each certificate. Otherwise, amendments shall not require a change in certificate policy object identifier.

9.13 DISPUTE RESOLUTION PROVISIONS

9.13.1 Disputes among Boeing, Affiliates, and Customers

Disputes shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

No stipulation

9.14 GOVERNING LAW

Subject to any limits appearing in applicable law, the laws of the State of Delaware, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Delaware, USA. This choice of law is made to ensure uniform procedures and interpretation for all participants, no matter where they are located.

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

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

9.15 COMPLIANCE WITH APPLICABLE LAW

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

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation

9.16.5 Force Majeure

To the extent permitted by applicable law, agreements among the parties shall include a force majeure clause protecting Boeing.

9.17 OTHER PROVISIONS

9.17.1 Order of Precedence.

Nothing herein shall operate to amend the terms of any separate signed agreement between or among The Boeing Company, a Relying Party, and a Customer. In the event of a conflict between the terms of any such agreement and this CP, the terms of the separate agreement shall prevail.

10 Certificate, CRL, and OCSP Formats

10.1 BOEING COMMERCIAL AIRLINE PKI AIRLINE PRIVATE CERTIFICATE AUTHORITY SIGNING CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 subject DN. These are self-signed, Airline-private Certificate Authorities. CN=<Airline Name> ESDD CA, OU=Boeing ESDD Hosted Service, O=<Formal Airline Organization Name>, C=<2 Letter Country for Airline>
Validity Period	20 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Same as Issuer
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or greater
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String
Subject Key Identifier	c=no; Octet String
Basic Constraints	c(ritical)=no; CA=True
Key Usage	c=yes; keyCertSign and, cRLSign are required, other values may be present.
Certificate Policies	c=no; Boeing OID for ESDD Hosted Certificate Policy: 1.3.6.1.4.1.73.15.3.6
Authority Information Access	Not Present
CRL Distribution Points	Not Present

10.2 AIRPLANE IDENTITY CERTIFICATE

This is the certificate issued to an Airplane once a CSR is issued and approved.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Subject DN of the Airline Issuer CA
Validity Period	1 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	<p>Subject DN of the Airplane, which includes:</p> <p>dnQualifier {2.5.4.46} = <a DN qualifier>, description {2.5.4.13} = <generic description>, UniqueIdentifier {2.5.4.45} = <A tail or registration number>, CN {2.5.4.3} = <Fully Qualified Domain Name, composed of the tail or registration number, and the airline specified DNS domain name. All components are separated by periods. OU {2.5.4.11} = Boeing ESDD Hosted Service, O {2.5.4.10} = <Full Airline Organization Name>, C {2.5.4.6} = <CountryCode></p> <p>Example:</p> <p>dnQualifier=0612130240, description=airplane, uniqueIdentifier=N234567, CN=N234567.aircraft.customerairlines.com, OU=B787, OU=Boeing ESDD Hosted Service, O=Customer Airlines Co. Ltd., C=US</p>
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or greater
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present

Field	Value
Issuer's Signature	sha-1WithRSAEncryption { 1 2 840 113549 1 1 5 } or sha256 WithRSAEncryption { 1 2 840 113549 1 1 11 }
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Basic Constraints	c(critical)=no; End entity=True
Key Usage	c=yes; digitalSignature is required, other values may be present.
Extended key usage	c=no; Both serverAuth and clientAuth are required, other values may be present.
Certificate Policies	c=no; Boeing OID 1.3.6.1.4.1.73.15.3.1.6
Subject Alternative Name	c=no; optional
Authority Information Access	id-ad-caIssuers access method entry contains HTTP URL for file containing current certificates issued to Issuing CA c=no; http://crl.boeing.com/<CA Name>.crl
CRL Distribution Points	always present; distributionPoint shall be the only field populated, and it shall contain an HTTP URI. The reason and crlIssuer fields shall not be populated. The CDP shall point to a full and complete CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer) c = no; http://crl.boeing.com/<CA Name>.crl

10.3 MAINTENANCE LAPTOP IDENTITY CERTIFICATES

For authenticating a maintenance laptop device and indicating its role as a “MaintenanceControlDisplay” when connected to the Airplane.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Subject DN of the Airline Issuer CA
Validity Period	1 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Subject DN of a Maintenance Laptop, which includes: description {2.5.4.13} = must be “CrewWirelessDevice”, UniqueIdentifier {2.5.4.45} = <An Airline specified asset identifier or unique name>, CN {2.5.4.3} = must be “MaintenanceControlDisplay” OU {2.5.4.11} = Boeing ESDD Hosted Service, O {2.5.4.10} = <Full Airline Organization Name>, C {2.5.4.6} = <CountryCode> Example: description=CrewWirelessDevice, uniqueIdentifier=<AirlinesUniqueIdentifier>, CN=MaintenanceControlDisplay, OU= Boeing ESDD Hosted Service,O=Customer Airlines Co. Ltd., C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or greater
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer’s Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value

Field	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Basic Constraints	c(ritical)=no; End entity=True
Key Usage	c=yes; digitalSignature is required, other values may be present.
Extended key usage	c=no; clientAuth is required
Certificate Policies	c=no; Boeing OID 1.3.6.1.4.1.73.15.3.1.6
Subject Alternative Name	c=no; optional
Authority Information Access	id-ad-caIssuers access method entry contains HTTP URL for file containing current certificates issued to Issuing CA c=no; http://crl.boeing.com/<CA Name>.crt
CRL Distribution Points	always present; distributionPoint shall be the only field populated, and it shall contain an HTTP URI. The reason and crlIssuer fields shall not be populated. The CDP shall point to a full and complete CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer) c = no; http://crl.boeing.com/<CA Name>.crl

10.4 APPLICATION IDENTITY (SSL) CERTIFICATES

For authenticating applications on the Airline network (for example, establishing authenticated SSL sessions). The application may be an SSL client or the SSL server.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Subject DN of the Airline Issuer CA
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Subject DN of an application or server name. This includes: CN=Fully Qualified DNS name or Unique Application Name, OU= Boeing ESDD Hosted Service, O=<Full Airline Organization Name>, C=<Country> Example: CN=Isaplibrarian.customerairlines.com, OU= Boeing ESDD Hosted Service, O=Customer Airlines Co. Ltd., C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or greater
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Basic Constraints	c(critical)=no; End entity=True
Key Usage	c=yes; digitalSignature is required, other values may be present.
Extended key usage	c=no; both clientAuth and serverAuth are required.

Field	Value
Certificate Policies	c=no; Boeing OID 1.3.6.1.4.1.73.15.3.1.6
Subject Alternative Name	c=no; optional, Host URL IP Address Host Name
Authority Information Access	<p>id-ad-caIssuers access method entry contains HTTP URL for file containing current certificates issued to Issuing CA</p> <p>c=no; http://crl.boeing.com/<CA Name>.crl</p>
CRL Distribution Points	<p>always present; distributionPoint shall be the only field populated, and it shall contain an HTTP URI. The reason and crlIssuer fields shall not be populated. The CDP shall point to a full and complete CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer)</p> <p>c = no; http://crl.boeing.com/<CA Name>.crl</p>

10.5 LSAP LIBRARIAN SUITE OBJECT SIGNING CERTIFICATES

Used by LSAP Librarian (LSAPL) Suite of tools for signing LSAP parts.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Subject DN of the Airline Issuer CA
Validity Period	Minimum 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Subject DN of the Signing Application and Organization, which includes: CN=<Unique Application Name>, OU = Boeing ESDD Hosted Service, O=<Full Airline Organization Name>, C=<Country> Example: CN=LSAP Approval, OU = Boeing ESDD Hosted Service, O=Customer Airlines Co. Ltd., C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Basic Constraints	c(ritical)=no; End entity=True
Key Usage	c=yes; digitalSignature is required; Other values may be present.

Field	Value
Extended key usage	c=no; No values required here, but CodeSigning may be present..
Certificate Policies	c=no; optional; {Issuer's CP OID n}
Subject Alternative Name	c=no; Boeing OID 1.3.6.1.4.1.73.15.3.1.6
Authority Information Access	<p>id-ad-caIssuers access method entry contains HTTP URL for file containing current certificates issued to Issuing CA</p> <p>c=no; http://crl.boeing.com/<CA Name>.crt</p>
CRL Distribution Points	<p>always present; distributionPoint shall be the only field populated, and it shall contain an HTTP URI. The reason and crlIssuer fields shall not be populated. The CDP shall point to a full and complete CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer)</p> <p>c = no; http://crl.boeing.com/<CA Name>.crl</p>

10.6 AIRLINE TRUSTED AGENT IDENTITY CERTIFICATES

Issued to persons that are explicitly authorized to submit certificate requests, enroll, approve, or otherwise communicate with the CA.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Subject DN of the Airline Issuer CA
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Subject DN of the Trusted Agent Windows Domain account
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or greater
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Basic Constraints	c(critical)=no; End entity=True
Key Usage	c=yes; digitalSignature is required, other values may be present.
Extended key usage	c=no; The Certificate Request Agent OID 1.3.6.1.4.1.311.20.2.1 is required, when using the AirplaneCSRTransform utility, and a Microsoft certificate authority;
Certificate Policies	c=no; Boeing OID 1.3.6.1.4.1.73.15.3.1.6
Subject Alternative Name	c=no; optional

Field	Value
Authority Information Access	id-ad-caIssuers access method entry contains HTTP URL for file containing current certificates issued to Issuing CA c=no; http://crl.boeing.com/<CA Name>.crt
CRL Distribution Points	always present; distributionPoint shall be the only field populated, and it shall contain an HTTP URI. The reason and crlIssuer fields shall not be populated. The CDP shall point to a full and complete CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer) c = no; http://crl.boeing.com/<CA Name>.crl

10.7 FULL AND COMPLETE CRL

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP Example CN=<Airline Name>ESDD CA <n>, OU=Boeing ESDD Hosted Service, O=Boeing, C=US
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	Value
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)

CRL Entry Extension	Value
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise

11 PKI Repository Interoperability Profile

Not applicable to Boeing Commercial Airline PKI

11.1 PROTOCOL

Not Applicable

11.2 AUTHENTICATION

Not Applicable

11.3 NAMING

Not Applicable

11.4 OBJECT CLASS

Not Applicable

11.5 ATTRIBUTES

Not Applicable

12 ACRONYMS & ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard

FAR	Federal Acquisition Regulations
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
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NSA	National Security Entity
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
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, Version 1
SSL	Secure Sockets Layer
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. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]

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 end entity is sometimes also called an "applicant" after applying to a 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 BCA 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. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
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. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Certificate	A digital representation of information which at least (1) identifies the certification authority 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 certification authority 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.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
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.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued 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, that 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. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
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]

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".
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	The entity that will be using the certificate.
Boeing Operational Authority (Boeing OA)	The Boeing Public Key Infrastructure Operational Authority is the organization selected by the Boeing 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 PKI CA and Operations.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
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. [NS4009]. 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.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
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. [NS4009] 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.
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.
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.
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.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
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.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	CAS personnel trusted and responsible to verify all airline certificate request information and interact with the PKI.

Trust Root 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.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
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. [NS4009]
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:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html .
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL

	Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
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.

15 ACKNOWLEDGEMENTS

Not applicable.