

The Boeing Company
Medium Assurance Domain
Certificate Policy

Version 10.1

February 29, 2012

PA Board approved: March 1, 2012

Signature Page

Kevin Murphy
Manager, IS IT Authentication Controls
Policy Authority Chairperson

DATE

Approval

by

Boeing PKI Policy Authority

Document

The Boeing Company Medium Assurance Domain Certificate Policy

Method of Approval (Signature/Roll Call Vote)	Date of Approval	Version Number	CRs Applied
Roll Call Vote	4/7/2006	Version 7.2.1	N/A
Roll Call Vote and e-mail	3/8/2007	Version 8.0	
Roll Call Vote and e-mail	4/12/2007	Version 8.0.4	03-12-07-01
Roll Call Vote	7/13/07	Version 9.0	CP_CR_06-07-07_03
Roll Call Vote	9/23/08	Version 9.1	CP_CR_09-05-08_03
Roll Call Vote	1/5/09	Version 9.2	CP_CR_11_21_08_01
Roll Call Vote	3/23/09	Version 9.3	CP_CR_3_17_09_01
Roll Call Vote	11/16/09	Version 9.4	CP_CR_11_10_09_01
Roll Call Vote	1/20/12	Version 10.0	Re-write for new infrastructure
Roll Call Vote	3/1/2012	Version 10.1	CP CR 2012_01

Table of Contents

1. INTRODUCTION	1
1.1 OVERVIEW	1
1.1.1 Certificate Policy (CP)	1
1.1.2 Relationship between the Boeing CP & the Boeing CPS	2
1.1.3 Scope	2
1.2 DOCUMENT IDENTIFICATION	3
1.3 PKI PARTICIPANTS	4
1.3.1 PKI Authorities	4
1.3.2 Other Participants	7
1.3.3 Applicability	7
1.4 CERTIFICATE USAGE	8
1.4.1 Appropriate Certificate Uses	8
1.4.2 Prohibited Certificate Uses	8
1.5 POLICY ADMINISTRATION	8
1.5.1 Organization administering the document	8
1.5.2 Contact Person	8
1.5.3 Person Determining Certification Practice Statement Suitability for the Policy	9
1.5.4 CPS Approval Procedures	9
1.5.5 Waivers	9
2. Publication & PKI Repository responsibilities	10
2.1 PKI REPOSITORIES	10
2.1.1 Boeing Repository Obligations	10
2.2 PUBLICATION OF CERTIFICATION INFORMATION	10
2.2.1 Publication of Certificates and Certificate Status	10
2.2.2 Interoperability	10
2.3 TIME OR FREQUENCY OF PUBLICATION	10
2.4 ACCESS CONTROLS ON PKI REPOSITORIES	10
3. Identification & Authentication	11
3.1 NAMING	11
3.1.1 Types of Names	11
3.1.2 Need for Names to Be Meaningful	11
3.1.3 Anonymity or Pseudonymity of Subscribers	11
3.1.4 Rules for Interpreting Various Name Forms	11

3.1.5	Uniqueness of Names.....	12
3.1.6	Recognition, Authentication, & Role of Trademarks	12
3.1.7	Name Claim Dispute Resolution Procedures	12
3.2	INITIAL IDENTITY VALIDATION.....	12
3.2.1	Method to Prove Possession of Private Key	12
3.2.2	Authentication of Organization Identity.....	12
3.2.3	Authentication of Individual Identity.....	12
3.2.4	Non-verified Subscriber Information.....	16
3.2.5	Validation of Authority.....	16
3.2.6	Criteria for Interoperation	17
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	17
3.3.1	Identification and Authentication for Routine Re-key.....	17
3.3.2	Identification and Authentication for Re-key after Revocation	17
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	17
4.	Certificate Life-Cycle Operational requirements.....	18
4.1	CERTIFICATE APPLICATION	18
4.1.1	Submission of Certificate Application	18
4.1.2	Enrollment Process and Responsibilities	19
4.2	CERTIFICATE APPLICATION PROCESSING.....	19
4.2.1	Performing Identification and Authentication Functions.....	19
4.2.2	Approval or Rejection of Certificate Applications.....	19
4.2.3	Time to Process Certificate Applications.....	20
4.3	ISSUANCE	20
4.3.1	CA Actions during Certificate Issuance	20
4.3.2	Notification to Subscriber of Certificate Issuance	20
4.4	CERTIFICATE ACCEPTANCE.....	20
4.4.1	Conduct constituting certificate acceptance	20
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.....	21
4.5.1	Subscriber Private Key and Certificate Usage	21
4.5.2	Relying Party Public key and Certificate Usage	21
4.6	CERTIFICATE RENEWAL.....	21
4.6.1	Circumstance for Certificate Renewal.....	21
4.6.2	Who may request Renewal.....	21

4.6.3	Processing Certificate Renewal Requests	22
4.6.4	Notification of New Certificate Issuance to Subscriber	22
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	22
4.6.6	Publication of the Renewal Certificate by the CA	22
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	22
4.7	CERTIFICATE RE-KEY.....	22
4.7.1	Circumstance for Certificate Re-key.....	22
4.7.2	Who May Request Certification of a New Public Key	22
4.7.3	Processing Certificate Re-Keying Requests.....	22
4.7.4	Notification of New Certificate Issuance to Subscriber	22
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	22
4.7.6	Publication of the Re-keyed Certificate by the CA.....	23
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	23
4.8	CERTIFICATE MODIFICATION	23
4.8.1	Circumstance for Certificate Modification.....	23
4.8.2	Who may request Certificate Modification.....	23
4.8.3	Processing Certificate Modification Requests	23
4.8.4	Notification of new certificate issuance to Subscriber.....	23
4.8.5	Conduct Constituting Acceptance of Modified Certificate	23
4.8.6	Publication of the Modified Certificate by the CA.....	23
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	23
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	24
4.9.3	Procedure for Revocation Request	24
4.9.4	Revocation Request Grace Period.....	25
4.9.5	Time within which CA must Process the Revocation Request.....	25
4.9.6	Revocation Checking Requirements for Relying Parties	25
4.9.7	CRL Issuance Frequency	25
4.9.8	Maximum Latency of CRLs.....	26
4.9.9	On-line Revocation Availability.....	26
4.9.10	On-line Revocation Checking Requirements.....	26
4.9.11	Other Forms of Revocation Advertisements Available	27
4.9.12	Special Requirements Related To Key Compromise	27
4.9.13	Circumstances for Suspension	27

4.9.14	Who can Request Suspension.....	27
4.9.15	Procedure for Suspension Request	27
4.9.16	Limits on Suspension Period.....	27
4.10	CERTIFICATE STATUS SERVICES	27
4.10.1	Operational Characteristics.....	27
4.10.2	Service Availability.....	27
4.10.3	Optional Features	27
4.11	END OF SUBSCRIPTION.....	27
4.12	KEY ESCROW & RECOVERY	27
4.12.1	Key Escrow and Recovery Policy and Practices	27
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	28
5.	Facility Management & Operations Controls.....	29
5.1	PHYSICAL CONTROLS.....	29
5.1.1	Site Location & Construction.....	29
5.1.2	Physical Access.....	29
5.1.3	Power and Air Conditioning	30
5.1.4	Water Exposures	30
5.1.5	Fire Prevention & Protection	30
5.1.6	Media Storage	30
5.1.7	Waste Disposal.....	30
5.1.8	Off-Site backup.....	30
5.2	PROCEDURAL CONTROLS.....	31
5.2.1	Trusted Roles	31
5.2.2	Number of Persons Required per Task.....	33
5.2.3	Identification and Authentication for Each Role.....	34
5.2.4	Roles Requiring Separation of Duties	34
5.3	PERSONNEL CONTROLS.....	34
5.3.1	Qualifications, Experience, and Clearance Requirements.....	34
5.3.2	Background Check Procedures	35
5.3.3	Training Requirements.....	35
5.3.4	Retraining Frequency and Requirements.....	36
5.3.5	Job Rotation Frequency and Sequence.....	36
5.3.6	Sanctions for Unauthorized Actions	36
5.3.7	Independent Contractor Requirements	36
5.3.8	Documentation Supplied To Personnel.....	36

5.4	AUDIT LOGGING PROCEDURES	36
5.4.1	Types of Events Recorded.....	37
5.4.2	Frequency of Processing Log	40
5.4.3	Retention Period for Audit Logs	40
5.4.4	Protection of Audit Logs.....	41
5.4.5	Audit Log Backup Procedures.....	41
5.4.6	Audit Collection System (internal vs. external)	41
5.4.7	Notification to Event-Causing Subject	41
5.4.8	Vulnerability Assessments	41
5.5	RECORDS ARCHIVE	42
5.5.1	Types of Records Archived.....	42
5.5.2	Retention Period for Archive	42
5.5.3	Protection of Archive.....	42
5.5.4	Archive Backup Procedures.....	43
5.5.5	Requirements for Time-Stamping of Records	43
5.5.6	Archive Collection System (internal or external).....	43
5.5.7	Procedures to Obtain & Verify Archive Information	43
5.6	KEY CHANGEOVER	43
5.7	COMPROMISE & DISASTER RECOVERY.....	44
5.7.1	Incident and Compromise Handling Procedures	44
5.7.2	Computing Resources, Software, and/Or Data Are Corrupted	45
5.7.3	Private Key Compromise Procedures	45
5.7.4	Business Continuity Capabilities after a Disaster	46
5.8	CA, CMS, AND RA TERMINATION.....	46
6.	Technical Security Controls	47
6.1	KEY PAIR GENERATION & INSTALLATION	47
6.1.1	Key Pair Generation	47
6.1.2	Private Key Delivery to Subscriber.....	48
6.1.3	Public Key Delivery to Certificate Issuer	48
6.1.4	CA Public Key Delivery to Relying Parties	49
6.1.5	Key Sizes.....	49
6.1.6	Public Key Parameters Generation and Quality Checking	49
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field).....	50
6.2	PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	50

6.2.1	Cryptographic Module Standards & Controls	50
6.2.2	Private Key Multi-Person Control	50
6.2.3	Private Key Escrow.....	50
6.2.4	Private Key Backup	51
6.2.5	Private Key Archival.....	51
6.2.6	Private Key Transfer into or from a Cryptographic Module	51
6.2.7	Private Key Storage on Cryptographic Module	52
6.2.8	Method of Activating Private Keys	52
6.2.9	Methods of Deactivating Private Keys.....	52
6.2.10	Method of Destroying Private Keys.....	52
6.2.11	Cryptographic Module Rating.....	52
6.3	OTHER ASPECTS OF KEY MANAGEMENT.....	52
6.3.1	Public Key Archival	52
6.3.2	Certificate Operational Periods/Key Usage Periods	52
6.4	ACTIVATION DATA	52
6.4.1	Activation Data Generation and Installation	52
6.4.2	Activation Data Protection.....	53
6.4.3	Other Aspects of Activation Data	53
6.5	COMPUTER SECURITY CONTROLS.....	53
6.5.1	Specific Computer Security Technical Requirements.....	53
6.5.2	Computer Security Rating.....	54
6.6	LIFE-CYCLE SECURITY CONTROLS	54
6.6.1	System Development Controls.....	54
6.6.2	Security Management Controls.....	54
6.6.3	Life Cycle Security Ratings	54
6.7	NETWORK SECURITY CONTROLS.....	55
6.8	TIME STAMPING.....	55
7.	Certificate, CARL/CRL, And ocsp profiles Format.....	56
7.1	CERTIFICATE PROFILE.....	56
7.1.1	Version Numbers	56
7.1.2	Certificate Extensions	56
7.1.3	Algorithm Object Identifiers.....	56
7.1.4	Name Forms.....	56
7.1.5	Name Constraints	58
7.1.6	Certificate Policy Object Identifier	58

7.1.7	Usage of Policy Constraints Extension	58
7.1.8	Policy Qualifiers Syntax & Semantics	58
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	58
7.2	CRL PROFILE	58
7.2.1	Version Numbers	58
7.2.2	CRL and CRL Entry Extensions	59
7.3	OCSP PROFILE	59
7.3.1	Version Number	59
7.3.2	OCSP Extensions	59
8.	Compliance Audit & Other Assessments	60
8.1	FREQUENCY OF AUDIT OR ASSESSMENTS	60
8.2	IDENTITY & QUALIFICATIONS OF ASSESSOR	60
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	60
8.4	TOPICS COVERED BY ASSESSMENT	60
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY	60
8.6	COMMUNICATION OF RESULTS	61
9.	Other Business & Legal Matters	62
9.1	FEES	62
9.1.1	Certificate Issuance/Renewal Fees	62
9.1.2	Certificate Access Fees	62
9.1.3	Revocation or Status Information Access Fee	62
9.1.4	Fees for other Services	62
9.1.5	Refund Policy	62
9.2	FINANCIAL RESPONSIBILITY	62
9.2.1	Insurance Coverage	62
9.2.2	Other Assets	62
9.2.3	Insurance/warranty Coverage for End-Entities	62
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	62
9.3.1	Scope of Confidential Information	62
9.3.2	Information not within the scope of Confidential Information	63
9.3.3	Responsibility to Protect Confidential Information	63
9.4	PRIVACY OF PERSONAL INFORMATION	63
9.4.1	Privacy Plan	63
9.4.2	Information treated as Private	63
9.4.3	Information not deemed Private	63

9.4.4	Responsibility to Protect Private Information.....	63
9.4.5	Notice and Consent to use Private Information	63
9.4.6	Disclosure Pursuant to Judicial/Administrative Process	63
9.4.7	Other Information Disclosure Circumstances	63
9.5	INTELLECTUAL PROPERTY RIGHTS	63
9.6	REPRESENTATIONS & WARRANTIES	63
9.6.1	Certification Authority Representations and Warranties	63
9.6.2	RA Representations and Warranties.....	64
9.6.3	Subscriber Representations and Warranties.....	64
9.6.4	Relying Parties Representations and Warranties	64
9.6.5	Representations and Warranties of other Participants	64
9.7	DISCLAIMERS OF WARRANTIES.....	64
9.8	LIMITATIONS OF LIABILITY	64
9.9	INDEMNITIES.....	65
9.10	TERM & TERMINATION.....	65
9.10.1	Term	65
9.10.2	Termination.....	65
9.10.3	Effect of Termination and Survival	65
9.11	INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS	65
9.12	AMENDMENTS	65
9.12.1	Procedure for Amendment.....	65
9.12.2	Notification Mechanism and Period.....	65
9.12.3	Circumstances under which OID must be changed.....	65
9.13	DISPUTE RESOLUTION PROVISIONS	65
9.14	GOVERNING LAW	66
9.15	COMPLIANCE WITH APPLICABLE LAW	66
9.16	MISCELLANEOUS PROVISIONS	66
9.16.1	Entire agreement	66
9.16.2	Assignment.....	66
9.16.3	Severability	66
9.16.4	Enforcement (Attorney Fees/Waiver of Rights)	66
9.16.5	Force Majeure	66
9.17	OTHER PROVISIONS	66
10.	Certificate, CRL and OCSP Formats	67
10.1	BOEING PCA TO CBCA CERTIFICATE.....	68

10.2 BOEING PCA SELF-SIGNED ROOT CERTIFICATE (ALSO CALLED TRUST ANCHOR).....	69
10.3 INTERMEDIATE OR SIGNING CA CERTIFICATE.....	70
10.4 MEDIUM HARDWARE SUBSCRIBER IDENTITY CERTIFICATE.....	71
10.5 MEDIUM SOFTWARE SUBSCRIBER IDENTITY CERTIFICATE.....	72
10.6 MEDIUM HARDWARE SUBSCRIBER SIGNATURE CERTIFICATE.....	73
10.7 MEDIUM SOFTWARE SUBSCRIBER SIGNATURE CERTIFICATE.....	75
10.8 MEDIUM HARDWARE SUBSCRIBER ENCRYPTION CERTIFICATE.....	76
10.9 MEDIUM SOFTWARE SUBSCRIBER ENCRYPTION CERTIFICATE.....	78
10.10 CODE SIGNING CERTIFICATE – PLACE HOLDER ONLY.....	79
10.11 MEDIUM HARDWARE DEVICE OR SERVER CERTIFICATE.....	80
10.12 MEDIUM SOFTWARE DEVICE OR SERVER CERTIFICATE.....	81
10.13 OCSP RESPONDER CERTIFICATE – PLACE HOLDER ENTRY ONLY.....	82
10.14 CRL FORMAT.....	83
Full and Complete CRL.....	83
10.15 OCSP REQUEST FORMAT – PLACE HOLDER ONLY.....	83
10.16 OCSP RESPONSE FORMAT – PLACE HOLDER ONLY.....	84
10.17 MEDIUM ASSURANCE RA ENROLLMENT AGENT CERTIFICATE PROFILE.....	85
10.18 MEDIUM ASSURANCE QUALIFIED SUBORDINATION CERTIFICATE PROFILE...87	87
10.19 MEDIUM ASSURANCE CA EXCHANGE CERTIFICATE PROFILE.....	88
10.20 MEDIUM ASSURANCE KEY RECOVERY AGENT (KRA)CERTIFICATE PROFILE..90	90
11.....	92
11.1 PROTOCOL.....	93
11.2 AUTHENTICATION.....	93
11.3 NAMING.....	93
11.4 OBJECT CLASS.....	93
11.5 ATTRIBUTES.....	93
12. ACRONYMS & ABBREVIATIONS.....	94
13. GLOSSARY.....	97
14. BIBLIOGRAPHY.....	105
15. ACKNOWLEDGEMENTS.....	106

1. INTRODUCTION

The Boeing Medium Assurance Domain (BMAD) is a PKI that accommodates programs that carry out or support the mission of The Boeing Company (Boeing) that require authentication, confidentiality, non-repudiation, and access control. These services are met with an array of network security components such as workstations, firewalls, routers, filters, proxy servers, encryption tools, and secured database and web servers. The operation of these components is supported and complemented by use of public key cryptography. Boeing does not sell certificates; rather PKI is used by the company to provide additional security to its business operations.

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

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

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

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

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

1.1.2 Relationship between the Boeing CP & the Boeing CPS

1.1.3 Scope

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

The following diagram represents the scope of the Boeing CP.

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

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

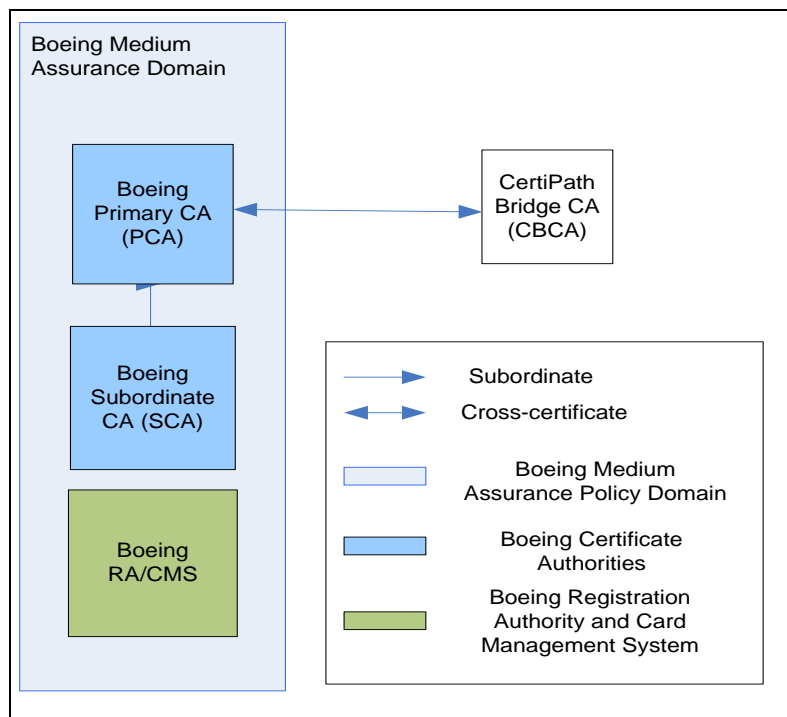
Certificates for end entities, such as Boeing employees, are issued from the Boeing Subordinate (SCA). This CA is subordinate to the Boeing Principal CA.

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

The Boeing Card Management System (CMS) is responsible for providing verified identities and information and manages the lifecycle of the smart cards.

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

Figure—Scope of Boeing CP



The scope of this CP in terms of subscriber (i.e., end entity) certificate types is limited to those listed in Section 10.

1.2 DOCUMENT IDENTIFICATION

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

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

The following diagram illustrates the Boeing OID structure.

id-boeing	::= { 1.3.6.1.4.73. }
id-security	::= { id-boeing 15 }
id-pki	::= { id-security 3 }
boeing-certificate-policies	::= { id-pki 1 }
id-mediumSoftware-SHA1	::= { boeing-certificate-policies 4 }
id-mediumHardware-SHA1	::= { boeing-certificate-policies 5 }
id-mediumCBPSoftware-SHA1	::= { boeing-certificate-policies 8 }
id-mediumCBPHardware-SHA1	::= { boeing-certificate-policies 9 }
Id-mediumHardware-cardAuthentication-SHA1	::= { boeing-certificate-policies 10 }
id-mediumSoftware-SHA256 – For future use	::= { boeing-certificate-policies 11 }
id-mediumHardware-SHA256 – For future use	::= { boeing-certificate-policies 12 }
id-mediumCBPSoftware-SHA256 – For future use	::= { boeing-certificate-policies 13 }
id-mediumCBPHardware-SHA256 – For future use	::= { boeing-certificate-policies 14 }
Id-mediumHardware-cardAuthentication-SHA256 – <i>For future use</i>	= { boeing-certificate-policies 15 }
id-mediumHardware-contentSigning-SHA1 – <i>For future use</i>	::= { boeing-certificate-policies 16 }

id-mediumHardware-contentSigning-SHA256 – <i>For future use</i>	={boeing-certificate-policies 17}
---	-----------------------------------

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

All of the requirements for “id-boeing...-SHA-256” are the same as those for the corresponding certificate policy OID without “SHA-256” in it except that the CAs not asserting “id-boeing...-SHA-256” may use SHA-1 for generation of PKI objects such as certificates and Certificate Revocation Lists (CRLs) after December 31, 2010.

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

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

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

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the CA.

1.3.1 PKI Authorities

1.3.1.1 Boeing Enterprise PKI Policy Authority (PA)

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

- Commission drafting and subsequent approval of this CP,
- Commission drafting, commission compliance analysis, and approval of any CPS associated with this CP,
- Commission drafting and approval of the application for cross certification with other authorities, such as the CertiPath Bridge Certificate Authority (CBCA),
- Reviewing the results of Certification Authority compliance audits to determine if the Certification Authorities are adequately meeting the stipulations of this CP and associated approved CPS documents, and make recommendations to the CAs regarding corrective actions, or other measures
- Determining the mappings between certificates issued by Boeing PCA and the levels of assurance set forth in the potential partner CPs, such as the CBCA CP (which shall include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the PA), and
- After an Entity is authorized to interoperate through the Boeing PCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the Boeing PCA.

A complete description of PA roles and responsibilities are provided in the Boeing Enterprise PKI PA Charter.

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

1.3.1.2 Boeing Operational Authority (OA)

The Boeing OA operates the Boeing PCA, the Boeing SCA, the Boeing Registration Authority (RA) and the Boeing Card Management System (CMS). Its duties include all operations required to issue medium assurance hardware certificates from the Boeing SCA, posting these certificates and Certificate Revocation List (CRLs) into the repository, and ensuring the availability of the repository to all relying parties. The Operational Authority acts upon approval of the PA. The OA activities are subject to review by the PA in order to ensure compliance with this CP and an applicable CPS.

1.3.1.3 Boeing Operational Authority Administrator (OAA)

The OA Administrator (OAA), appointed by and reporting to the PA Chair, is the individual within the OA who has principal responsibility for overseeing the proper operation of the CA and its repositories. The OAA appoints individuals to the position Operational Authority Officer (OAO).

1.3.1.4 Boeing Operational Authority Officers (OAO)

These officers are the individuals within the Operational Authority, selected by the Administrator (OAA), who operate the Boeing CAs and the Boeing PKI Repository including executing the PA direction to issue certificates to CAs or taking other action to affect interoperability between the Boeing Principal CA and other CAs. The roles in the Operational Authority can be found in section 5.2.1. The Boeing Operational Authority Officer (OAO) issues certificates to subordinate CAs and cross certificates when required.

1.3.1.5 Boeing Principal CA (PCA)

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

1.3.1.6 Boeing Subordinate CA (SCA)

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

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Rekey of signing material

- Ensuring that all aspects of the SCA services, operations, and infrastructure related to certificates issued are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7 Boeing Certificate Status Authority (CSA)

The CSA provides status of certificates or certification paths. Examples of CSA are:

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates.
- OCSP Responders that are keyless and simply repeat responses signed by other Responders adhere to the same security requirements as repositories.

Boeing has not yet implemented a CSA, so this entry is being made as a placeholder only at this time. All other sections in this CP relating to the CSA will be omitted or noted with "No stipulation until a Boeing CSA is implemented".

1.3.1.8 Card Management System (CMS)

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

1.3.1.9 Registration Authority (RA)

The Registration Authority for the Boeing CAs is responsible for identification and authentication of certificate subjects, but it does not sign or issue certificates. The RA is responsible for but not limited to the following functions:

- Records the identification and authentication process
- Control over certificate issuance
- Interfacing with the CA for certificate issuance and revocation

1.3.1.10 Subscribers

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

1.3.1.11 Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in

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

1.3.2 Other Participants

1.3.2.1 Related Authorities

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

1.3.2.2 Trusted Agent

A Trusted Agent is the entity that collects and verifies each Subscriber's identity information on behalf of the RA. A Trusted Agent does not have privileges on the CA to enter or approve subscriber information.

1.3.2.3 PKI Sponsor

The PKI sponsor serves as the applicant and subscriber on behalf of a non-human applicant or subscriber, such as a device or piece of software.

1.3.2.4 Key Recovery Agents

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

1.3.3 Applicability

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

To provide sufficient granularity, this CP specifies security requirements for the assurance levels listed in Section 1.2.

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

Assurance Level	Applicability
Medium-software or Medium-CBP-software	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private

	keys are stored in software at this assurance level.
Medium-hardware or Medium-CBP-hardware	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber private keys are stored in hardware such as a smart card or a hardware secure device, at this assurance level.

1.3.3.1 Factors in Determining Usage

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

1.3.3.2 Obtaining Certificates

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

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

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

1.4.2 Prohibited Certificate Uses

Certificate usage not identified in Section 1.4.1 is prohibited.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

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

1.5.2 Contact Person

The Boeing Company

Attn: Boeing Enterprise PKI Policy Authority Chair
P.O. Box 3707
MC 7L-07
Seattle, WA 98124-2207

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

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

In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. The compliance auditor shall be from a firm which is independent from the entity being audited. The compliance auditor may not be the author of the subject CPS. The Boeing Enterprise PKI PA shall determine whether a compliance auditor meets these requirements.

1.5.4 CPS Approval Procedures

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. A Boeing CPS which is contained in a separate document published by the Boeing Operational Authority and approved by the Boeing PA specifies how this CP and any Memoranda of Agreements that the Boeing PA has approved shall be implemented to ensure compliance with their provisions for its respective CA.

1.5.5 Waivers

The Boeing Enterprise PKI PA does not issue waivers to CAs asserting compliance to this policy.

2. PUBLICATION & PKI REPOSITORY RESPONSIBILITIES

2.1 PKI REPOSITORIES

The Boeing Operational Authority (OA) shall operate repositories to support Boeing PKI operations. Repositories are used to hold information needed by an internal user of the Boeing PKI. They are also used by external users to support interoperability with other organizational PKI domains that employ the CertiPath Bridge CA for this purpose.

2.1.1 Boeing Repository Obligations

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

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The Boeing Operational Authority shall publish information concerning the Boeing PCA and the Boeing SCA necessary to support its use and operation. A copy of this Certificate Policy shall be publicly available on the Boeing website (see <http://crl.boeing.com/crl/>)

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

- CA certificates asserting this policy
- CRLs

2.2.2 Interoperability

No stipulation beyond Section 2.1.

2.3 TIME OR FREQUENCY OF PUBLICATION

See Section 4.

2.4 ACCESS CONTROLS ON PKI REPOSITORIES

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

3. IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

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

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

3.1.2 Need for Names to Be Meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must meaningfully identify the assigned subscriber..

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

All DNs shall accurately reflect organizational structures. When User Principal Name (UPN) is used, it shall accurately reflect organizational structure.

The CAs asserting one or more of the policies in this CP shall only sign certificates with subject names from within a name-space approved by the Boeing PA. In the case where one CA certifies another CA, the certifying CA must impose restrictions on the name space authorized in the subordinate CA, which are at least as restrictive as its own name constraints.

Boeing reserves the right to assert name constraints in CA certificates issued by the Boeing CA in order to limit the name space of the subject CAs to name spaces that are appropriate for subject CA domains.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile in Section 10. The Boeing Operational Authority (OA) shall be the authority responsible for CA name control space.

3.1.5 Uniqueness of Names

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

The Boeing CA shall document in its applicable CPS:

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

3.1.6 Recognition, Authentication, & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution Procedures

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the CA. The CA shall then validate the signature using the party’s public key. The PA may allow other mechanisms that are at least as secure as those cited here.

3.2.2 Authentication of Organization Identity

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

3.2.3 Authentication of Individual Identity

For subscribers, the Boeing CMS shall ensure that the subscriber’s identity information is verified and checked in accordance with this CP and the applicable CPS. The RA shall ensure that the applicant’s identity information and public key are bound.

Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance

and shall be addressed in the applicable CPS. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification;
- A signed declaration by that person that he or she verified the identity of the applicant as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this Certificate Policy;
- To provide proof of the country of citizenship, the applicant shall present one valid National Government-issued photo ID (e.g. passport, naturalization papers, certificate of citizenship), or two valid non-National Government IDs, (e.g., birth certificate) plus a recent photo ID (e.g., Drivers License). To provide their organizational affiliation, the applicant must present their Boeing badge with photo imprint.
- Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note: Examples of signatures equivalent to handwritten signature are a good fingerprint or other adequate biometric that can be linked to the individual identity. Another example of a signature equivalent to handwritten signature is digital signature that can be verified using a certificate provided to the same identity. However, that certificate must not be the same certificate for whose issuance the identity proofing is being performed.

Identity shall be established by in-person proofing before the Trusted Agent; information provided shall be verified to ensure legitimacy. Requirements for authentication of individual identity using an in-person antecedent are listed in Section 3.2.3.3

3.2.3.1 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) shall be named as certificate subjects. In such cases, the component must have a human sponsor. The PKI sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or the CMS to communicate with the PKI sponsor when required.

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

- Verification of digitally signed messages sent from the PKI Sponsor (using certificates of equivalent or greater assurance than that being requested)
- In-person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3

3.2.3.2 Human Subscriber Re-Authentication

If human subscriber credentials containing the private keys associated with the public key certificates are lost, damaged, or stolen, the subscriber may be issued new certificates using the process described in this section. However, the validity period of the certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1. Alternatively, the subscriber can undergo an initial identity proofing process described in Section 3.2.3.3.

The applicable CA or RA shall ensure that the subscriber's identity information and public key are properly bound. Additionally, the CA or RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification;
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy which may be met by establishing how the subscriber is known to the verifier as required by this Certificate Policy;
- The subscriber shall present one valid National Government-issued photo ID (e.g. passport) or valid non-National Government issued photo ID (e.g., Drivers License). To provide their organizational affiliation, the applicant must present their Boeing Badge with photo imprint.
- Unique identifying numbers from the Identifier (ID) of the verifier and from the ID of the subscriber;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or equivalent and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

The process documentation and authentication requirements may include a good fingerprint match or other adequate biometric from the Subscriber with the biometric stored in an authoritative trusted database. This database shall be protected as stipulated in Section 4.3 of this CP.

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

3.2.3.3 Human Subscriber Initial Identity Proofing Via Antecedent Relationship

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

1. Certificate Applicant shall personally appear before an RA or a Trusted Agent;
2. The Certificate Applicant and the Identity Verifier (i.e., RA and Trusted Agent) shall have an established working⁹ relationship with the Certificate Sponsor (i.e. The Boeing Company). The relationship shall be sufficient enough to enable the Identity Verifier to, with a high degree of certainty, verify that the Certificate Applicant is the same person that was identity proofed. An example to meet this requirement is when the Certificate Applicant, RA, and Trusted Agents are employed by the same company and the company badge forms the basis for the Certificate Applicant authentication;
3. The Certificate Applicant shall present a valid Boeing Company issued badge. This photo ID shall have been issued on the basis of in-person identity proofing using one valid Federal Government-issued Picture I.D. (e.g. Passport), or two valid Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License);
4. The Identity Verifier shall record the following:
 - a) His/her own identity;
 - b) Unique identifying number from the Identifier (ID) of the Identity Verifier;
 - c) Unique identifying number from the Certificate Sponsor-issued photo ID to the Certificate Applicant;
 - d) Date and time of the identity verification; and
 - e) Date and time of Sponsor-issued photo ID, if applicable.
5. The Identity Verifier shall sign a declaration that he or she verified the identity of the Certificate Applicant as required by the applicable certificate policy which may be met by establishing how the Certificate Applicant is known to the Identity Verifier as required by this certificate policy; and
6. The Certificate Applicant shall sign a declaration of identity using a handwritten signature or equivalent using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. This declaration shall be signed in the presence of the Identity Verifier.

3.2.3.4 Authentication of Human Subscriber for Role Certificates

Subscribers may be issued role certificates. A role certificate shall identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificate can be used in situations where non-repudiation is desired. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time, however, the signature key pair

⁹ An example of "established working relationship" is the person is employed by the Certificate Sponsor (i.e. The Boeing Company). Another example of an "established working relationship" is the person is employed as a contractor of the Certificate Sponsor (i.e. The Boeing Company).

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

Subscribers receiving role certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). For the role signature certificate, the individual assigned the role or the role sponsor may act on behalf of the certificate subject for certificate management activities such as renewal, re-key and revocation. Issuance and modification of role signature certificate shall require the approval of the role sponsor. Rekey and renewal of role signature certificate shall require the approval of the role sponsor if the validity period is extended beyond that already approved by the role sponsor. For the role encryption certificate, only the role sponsor may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

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

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

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

3.2.4 Non-verified Subscriber Information

Unverified information shall not be included in certificates.

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

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

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

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

3.3.1 Identification and Authentication for Routine Re-key

The CA and subscribers shall be authenticated through use of their current public key certificates or by using the initial identity-proofing process as described in Section 3.2. . For end entities with medium-software, medium-CBP-software, medium hardware, and medium-CBP-hardware assurance certificates, the in-person identity-proofing process needs to be carried out once every nine (9) years.

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

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

3.3.2 Identification and Authentication for Re-key after Revocation

To obtain a new certificate after a certificate has been revoked, the certificate subject shall be authenticated through use of another current, valid public key certificate in accordance with Section 3.3.1 or by using the in-person identity-proofing process as described in Section 3.2.3.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests shall be authenticated.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

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

4.1 CERTIFICATE APPLICATION

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

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

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

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

4.1.1 Submission of Certificate Application

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

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

For subscriber certificates, the application shall be submitted by an authorized prospective subscriber in the case of human subscribers, or an authorized PKI sponsor in the case of components

4.1.2 Enrollment Process and Responsibilities

External CAs applying for cross certificates with the Boeing PCA shall submit a request for cross-certification to the Boeing PA accompanied by their CP. The Boeing PA shall require a CP/CPS compliance analysis and pre-operational audit, from a third-party auditor, as described in section 8. The Boeing PA shall perform a certificate policy mapping to validate policy assurance levels are equivalent. Upon issuance, each cross-certificate issued by the Boeing PCA shall be manually checked to ensure each field and extension is properly populated with the correct information, before the certificate is delivered to the Subject CA.

Boeing CAs shall submit a request to the Boeing PA, accompanied by their CPS. The Boeing PA shall evaluate the submitted CPS for acceptability. The PA may require an initial compliance analysis and pre-operational audit, performed by parties of the PA's choosing, to ensure that the CA is in compliance with this CP, prior to the PA authorizing the PCA to issue a certificate to an SCA and authorizing the SCA to issue and manage certificates asserting a policy OID from this CP.

The PCA shall only issue certificates to subordinate CAs upon receipt of written authorization from the PA.

CAs shall issue certificates asserting a policy OID from this CP only upon receipt of written authorization from the Boeing PA, and then may do so only within the constraints imposed by the PA or its designated representatives.

4.2 CERTIFICATE APPLICATION PROCESSING

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

4.2.1 Performing Identification and Authentication Functions

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

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

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

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

Subscribers are expected to present proof of identity in person to Trusted Agents, to electronically agree to the subscriber agreement, as well as to sign it with a handwritten signature.

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

The entire registration process for subscribers (i.e., from acceptance of initial application to identity proofing to certificate) shall take no more than 30 days.

4.3 ISSUANCE

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

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

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

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

4.3.1 CA Actions during Certificate Issuance

A CA shall verify the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA shall post the certificate as set forth in this CP.

4.3.2 Notification to Subscriber of Certificate Issuance

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

4.4 CERTIFICATE ACCEPTANCE

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

4.4.1 Conduct constituting certificate acceptance

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

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

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

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Boeing OA shall inform the Boeing PA of any CA certificate issued by the Boeing Principal CA.

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

Notification of cross certificate issuance by the Boeing PCA shall be provided to all cross-certified entities.

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

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

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

Subscribers and CAs shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

4.5.2 Relying Party Public key and Certificate Usage

Relying parties shall use public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 CERTIFICATE RENEWAL

Boeing does not support certificate renewal.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who may request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 CERTIFICATE RE-KEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys and re-establish their identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

4.7.1 Circumstance for Certificate Re-key

A CA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a certificate.

4.7.2 Who May Request Certification of a New Public Key

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

A PKI Sponsor may request may request re-key of component certificate.

4.7.3 Processing Certificate Re-Keying Requests

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

- In-person registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3

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

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1

4.7.6 Publication of the Re-keyed Certificate by the CA

See section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3

4.8 CERTIFICATE MODIFICATION

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

4.8.1 Circumstance for Certificate Modification

Not Applicable

4.8.2 Who may request Certificate Modification

Not applicable

4.8.3 Processing Certificate Modification Requests

Not Applicable

4.8.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9 CERTIFICATE REVOCATION & SUSPENSION

Revocation requests must be authenticated.

4.9.1 Circumstances for Revocation of a Certificate

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

- Identifying information or affiliation components of any names in the certificate becomes invalid before the certificate expires.
- The subscriber's employment is terminated or Subscriber is suspended for cause.

- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- The private key is suspected of compromise.
- The subscriber or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked.

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

4.9.2 Who Can Request Revocation of a Certificate

Any Boeing SCA certificate may be revoked upon direction of the Boeing Policy Authority. In the case of cross certified CAs, the certificate shall be revoked upon direction of the Boeing PA at the request of an official or officials identified in the governing agreement as authorized to make such a request.

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

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

4.9.3 Procedure for Revocation Request

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

Any CA may unilaterally revoke another CA certificate it has issued. However, the Boeing OA for a Boeing CA shall revoke a Subject CA certificate only in the case of an emergency. Generally, the certificate shall be revoked based on the subject request, authorized representative of subject request, or Boeing PA request.

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the certificate. In the case of a CA certificate issued by a Boeing CA, the Boeing OA shall seek guidance from the Boeing PA before revocation of the certificate except when the Boeing PA is not available and there is an emergency situation such as:

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

For cross-certified CA, the Boeing PA Chair shall direct the Boeing OA in writing to revoke the CA certificate. Upon revocation of the certificate, the OA shall post an updated CRL to the appropriate repository, in accordance with section 2.2.1.

At the medium-hardware, medium-CBP-hardware assurance levels, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the unretrieved tokens shall be immediately revoked for the reason of key compromise.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within which CA must Process the Revocation Request

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

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

Assurance Level	Processing Time for Revocation Requests
Medium Software and Medium CBP Software	Within 18 hours of receipt of request
Medium Hardware and Medium CBP Hardware	Within 18 hours of receipt of request

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

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

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

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

CRL Issuance Frequency	
Routine	At least once every 30 days for Off-line Roots and Off-line Bridge CAs; At Least Once every 24 hours for all others
Loss or Compromise of Private Key	Within 18 Hours of Notification
CA Compromise	Immediately, but no later than within 18 hours after Notification

The CAs that issue routine CRLs less frequently than the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs. Such CAs shall also be required to notify the Boeing PA upon Emergency CRL issuance. The Boeing PA shall in turn notify the CertiPath Operational Authority and all cross certified CAs of revocation.

4.9.8 Maximum Latency of CRLs

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

4.9.9 On-line Revocation Availability

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

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

4.9.10 On-line Revocation Checking Requirements

CAs are not required to operate a CSA covering the certificates they issue. Boeing operates in some environments that cannot accommodate on-line communications, so all CAs shall be required to support CRLs..

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.11.1 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in section 4.9.7.

4.9.13 Circumstances for Suspension

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

4.9.14 Who can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

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

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW & RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

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

This CP requires a Boeing SCA to escrow decryption private keys (see Section 6.2.3). Boeing key escrow and recovery capability shall be governed by the CertiPath Key Recovery Policy (KRP). The method, procedures and controls which will apply to key recovery shall be described in a Key Recovery Practice Statement (KRPS) that has been paired with the KRP.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5. FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location & Construction

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA and CMS Equipment

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

- Ensure that no unauthorized access to the hardware is permitted,
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers,
- Be monitored for unauthorized intrusion at all times,
- Ensure an access log is maintained and inspected periodically,
- Provide at least three layers of increasing security (e.g. perimeter, building, and equipment room),
- Require two-person physical access control to both the cryptographic module and computer system.

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA or CMS equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module.

A security check of the facility housing CA and CMS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed,” and for a CA, that all equipment other than the repository is shut down),
- Any security containers are properly secured,
- Physical security systems (e.g., door locks, vent covers) are functioning properly,
- The area is secured against unauthorized access.

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

5.1.2.2 Physical Access for RA Equipment

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

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention & Protection

No stipulation.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the applicable CPS. Backups are to be performed and stored offsite not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

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

The requirements of this policy are drawn in terms of four roles (*Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile*):

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

The following sections define these and other trusted roles.

5.2.1.1 CA Administrator and Certificate Manager

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys.

Administrators do not issue certificates to subscribers.

Certificate Manager

Manages the lifecycle of the certificates. Approve and revoke certificates.

Under Microsoft Role Separation the Certificate Manager has rights to do the following:

- Issue and approve certificates
- Deny certificates
- Revoke certificates
- Reactivate certificates placed on hold
- Renew certificates

5.2.1.2 Officer

Any officer that operates under this policy is subject to the stipulations of this policy. The officer's role and the corresponding procedures shall be defined in a CPS. The Officer's responsibility is to ensure the following functions occur according to the stipulations of this policy, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Audit Administrator

The audit administrator role is responsible for:

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

5.2.1.4 Operator

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

5.2.1.5 Registration Authority

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2
- Accepting/entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from a CA;
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6 Certificate Status Authority (CSA) Roles

No stipulation until Boeing implements a CSA at a future date.

5.2.1.7 Card Management System (CMS) Roles

A CMS shall have at least the following roles.

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

- A CMS Audit Administrator who shall be responsible for:
 - Reviewing, maintaining, and archiving audit logs; and
 - Performing or overseeing internal compliance audits to ensure that the CMS is operating in accordance with its CPS.
- A CMS Operator who shall be responsible for:
 - The routine operation of the CMS equipment; and
 - Operations such as system backups and recovery or changing recording media.

5.2.1.8 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.1 and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A PKI Sponsor need not be a trusted role, but should have been issued a credential that is equal to or higher assurance level than the credential that they are sponsoring.

5.2.1.9 Trusted Agent

A Trusted Agent is responsible for:

- Verifying identity, pursuant to section 3.2.3; and
- Securely communicating subscriber information to the RA.

5.2.1.10 Key Recovery Agents

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

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

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

5.2.2 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 signing key activation;

- 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 as defined in Section 5.2.1.

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

All roles are recommended to have multiple persons in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

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

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

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

No individual shall be assigned more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each CA and CMS shall be identified. The trusted roles of these individuals per Section 5.2.1 shall be identified.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, shall be subject to background investigation and must be U.S. citizens. Personnel appointed to trusted roles (including CA trusted roles, CMS trusted roles, roles, Trusted Agent, and RA role) shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the trusted role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;

- Have not been denied a security clearance, or had a security clearance revoked;
- Have a U.S. Secret or higher security clearance;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority.

5.3.2 Background Check Procedures

All persons filling trusted roles (including CA trusted roles, CMS trusted roles, Trusted Agent, and RA role), shall have completed a favorable background investigation. The scope of the background check shall include the following areas covering the past five years and should be refreshed every five years:

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

One way to meet these requirements of this section is to have a national agency security clearance that is based on a five year background investigation.

Practice Note: Interim clearance may be acceptable. However, if the final adjudication is not favorable, all certificates issued while the person had a trusted role may require re-evaluation and possibly revocation.

If the person has been in the work force less than five years, the employment verification shall consist of the periods during which the person has been in the work force.

5.3.3 Training Requirements

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

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

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

- CA Subscriber requirements during personal appearance; Process for encoding Boeing SecureBadge with Medium Assurance Certificates.
- RA security principles and mechanisms
- Boeing security and operational policies and procedures;
- Ethics training;
- Incident and compromise reporting and handling.

5.3.4 Retraining Frequency and Requirements

The OA shall ensure that all individuals responsible for PKI roles shall be aware of changes in the CA, CMS and RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, CMS hardware or software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Contract employees at Boeing are held to the same functional and security criteria that apply to a Boeing Employee in a comparable position. Contract employees shall not serve in any trusted roles.

5.3.8 Documentation Supplied To Personnel

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

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.4 AUDIT LOGGING PROCEDURES

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

defined in this section shall be maintained in accordance with Section 5.5.2, Retention Period for Archive

5.4.1 Types of Events Recorded

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

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

Auditable events shall include:

Auditable Event	CA	CMS	RA
SECURITY AUDIT			
Any changes to the Audit logging parameters, e.g., audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X
Obtaining a third-party time-stamp	X	X	X
IDENTITY-PROOFING			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of <i>maximum number of authentication attempts</i> is changed	X	X	X
The number of unsuccessful authentication attempts exceeds the <i>maximum authentication attempts</i> during user login	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X
LOCAL DATA ENTRY			
All security-relevant data that is entered in the system	X	X	X
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT			

Auditable Event	CA	CMS	RA
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X
KEY GENERATION			
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of Component private keys	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	X	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X
SECRET KEY STORAGE			
The manual entry of secret keys used for authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT			
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All certificate requests	X	X	X
CERTIFICATE REVOCATION			
All certificate revocation requests	X	X	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request	X	X	N/A
CA CONFIGURATION			
Any security-relevant changes to the configuration of the Component	X	X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	X	N/A
The access control privileges of a user account or a role are modified	X	X	N/A
CERTIFICATE PROFILE MANAGEMENT			
All changes to the certificate profile	X	X	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT			

Auditable Event	CA	CMS	RA
All changes to the CSA profile (e.g. OCSP profile)	N/A	N/A	N/A
REVOCACTION PROFILE MANAGEMENT			
All changes to the revocation profile	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			
All changes to the certificate revocation list profile	X	N/A	N/A
MISCELLANEOUS			
Appointment of an individual to a Trusted Role	X	X	X
Designation of personnel for multiparty control	X	X	N/A
Installation of the Operating System	X	X	X
Installation of the PKI Application	X	X	X
Installation of hardware cryptographic modules	X	X	X
Removal of hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System Startup	X	X	X
Logon attempts to PKI Application	X	X	X
Receipt of hardware / software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Back up of the internal CA database	X	X	N/A
Restoration from back up of the internal CA database	X	X	N/A
File manipulation (e.g., creation, renaming, moving)	X	-	-
Posting of any material to a PKI Repository	X	-	N/A
Access to the internal CA database	X	-	N/A
All certificate compromise notification requests	X	X	X
Loading tokens with certificates	X	X	X
Shipment of Tokens	X	X	X
Zeroizing and Destroying Tokens	X	X	X
Re-key of the Component	X	X	X
CONFIGURATION CHANGES			
Hardware	X	X	-
Software	X	X	X
Operating System	X	X	X

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

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every 30 days for CMS, RA and all on-line CAs and at least once every 90 days for all off-line CAs or whenever an off-line CA is powered up, whichever comes first. A statistically significant sample of security audit data generated by the CA, CMS or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The Audit Administrator shall explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite for at least 60 days in addition to being retained in the manner described below. The Audit Administrator shall be the only person responsible to

manage the audit logs (e.g., review, backup, rotate, delete, etc.) of the CA and CMS system. For RA systems, a system administrator other than the RA shall be responsible for managing the audit logs.

5.4.4 Protection of Audit Logs

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

- Only authorized people¹⁰ have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

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

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up every 30 days. A copy of the audit log shall be sent off-site on a monthly basis.

5.4.6 Audit Collection System (internal vs. external)

Audit processes shall be invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed and the integrity of the system or confidentiality of the information protected by the system is at risk, a determination shall be made by the OA whether to suspend operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

CA Administrator, System Administrator, and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system and the card management system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the Audit Administrator for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data. The Audit Administrator shall document the summary results of the period review of the audit logs. The OA shall perform routine self-assessments of security controls.

¹⁰ For the CA and CSA, the authorized individual shall be the Audit Administrator. For the RA system, the authorized individual shall be a system administrator other than the RA.

5.5 RECORDS ARCHIVE

5.5.1 Types of Records Archived

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

Data To Be Archived	CA	CMS	RA
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	-
Modifications and updates to system or configuration	X	X	-
Certificate requests	X	X	-
Revocation requests	X	X	-
Subscriber identity authentication data as per Section 3.2.3	X	X	X
Documentation of receipt and acceptance of certificates	X	X	X
Documentation of receipt of Tokens	X	X	X
All certificates issued or published	X	X	N/A
Record of Component CA Re-key	X	X	X
All CRLs and CRLs issued and/or published	X	N/A	N/A
All Audit Logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 10 years and 6 months for Medium Assurance levels.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA, CMS and RA, the authorized individuals are Audit Administrators. The contents of the archive shall not be released except as determined by the Boeing PA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CMS,

or RA) with physical and procedural security controls equivalent or better than those for component.

5.5.4 Archive Backup Procedures

N/A.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (internal or external)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain & Verify Archive Information

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

5.6 KEY CHANGEOVER

A CA uses a signing (private) key for creating certificates; however, relying parties employ the CA certificate for the life of the Subscriber certificate beyond that signing. Therefore, CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys, and the CA certificate validity period must extend one Subscriber certificate validity period (listed in Section 3.3) past the last use of the CA private key.

To minimize risk to the PKI through compromise of a CAs key, the private signing key shall be changed more frequently, and only the new key shall be used for certificate signing purposes from that time. The older, but still valid, certificate shall be available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected. For a thorough discussion of key changeover, see Certificate Management Protocol [RFC2510]. For additional constraints on certificate life and key sizes, see Section 6.1.5

The following table provides the life times for certificates and associated private keys.

Key	2048 Bit Keys	
	Private Key	Certificate
Boeing PCA G2 Root CA	10 years	20 years
Boeing SecureBadge Medium G2 Signing CA	5 years	10 years

Boeing Medium Subscriber Identity or Signature	3 years	3 years
Boeing Medium Subscriber Encryption	3 years	3 years
Boeing Medium Card Authentication	3 years	3 years
Code Signer	5 years	5 years
Device	3 years	3 years

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

The Boeing PA members shall be notified if any of the following cases occur:

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

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

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

The Boeing OA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

When Boeing has detected an incident or compromise of the Boeing Root CA (PCA) and/or Boeing Subordinate Signing CA (SCA), and upon approval by the Boeing CISO, the Boeing PA Chair shall notify all cross certified PKIs.

The above measures will allow member entities to protect their interests as Relying Parties.

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

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

If the CA or CMS equipment is damaged or rendered inoperative, but the signature keys are not destroyed, operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The Boeing PA shall be notified as soon as possible.

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

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued certificates by the CA shall be securely¹¹ notified immediately. This will allow other CAs to protect their subscribers' interests as Relying Parties. The CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS. If revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

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

1. All cross certified CAs shall be securely notified at the earliest feasible time (so that entities may issue CRLs revoking any cross-certificates issued to the CA);
2. A CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
3. New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
4. If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the notAfter date in the certificate as in original certificates; and
5. If the CA is the Root CA, it shall provide the Subscribers the new trust anchor using secure means.

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

¹¹ With confidentiality, source authentication, and integrity security services applied.

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

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

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

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PA shall be notified at the earliest feasible time, and the PA shall direct the OA to revoke the CA certificates, and direct the CA to follow the procedures outlined in section 5.7.3.

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

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

5.8 CA, CMS, AND RA TERMINATION

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

In the event of a CA termination, Boeing shall provide as much advance notice as circumstances permits to all cross certified CAs prior to the termination.

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

The CA, CMS, and RA shall destroy all its private keys upon termination.

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

If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the CA.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation

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

Entity	FIPS 140-1/2 Level	Hardware or Software	Same Module
CA	3	Hardware	Same
CMS	3	Hardware	Same
RA	2	Hardware	Same
Code Signing	2	Hardware	Same
Content Signing	2	Hardware	Same
End Entity Signature or Authentication (medium-software and medium-CBP-software)	1	Software	No Requirement
End Entity Encryption (medium-software and medium-CBP-software)	1	Software	No Requirement
End Entity Signature or Authentication (medium-hardware, medium-CBP-hardware)	2	Hardware	Same
End Entity Encryption (medium-hardware, medium-CBP-hardware)	2	Hardware	No Requirement
Server (medium-software and medium-CBP-software)	1	Software	No Requirement
Server (medium-hardware, medium-CBP-hardware)	2	Hardware	Same

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

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

Multiparty control shall be used CA key pair generation, as specified in Section 5.2.2.

CA key pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third party

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

6.1.2 Private Key Delivery to Subscriber

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

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

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

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

The CA or the CMS shall maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

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

- Where key pairs are generated by the Subscriber or CMS, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance.

- The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

If the Boeing PA determines that the security of a particular algorithm may be compromised, it may require the CAs to revoke the affected certificates. All certificates (including self-signed certificates), CRLs and other protocols used by the PKI (e.g., Transport Layer Security (TLS)) shall use the following algorithm suites:

Public keys in CA, Identity, Authentication, and Digital Signature Certificates; CRL Signatures;	2048 bit RSA
Public Keys in Encryption Certificates (PKCS 1 for RSA and NIST SP 800-56A for ECDH)	2048 bit RSA
Symmetric Encryption	3 Key TDES or AES
Hashing Algorithm for Certificates	SHA-1
Hashing Algorithm for CRLs	SHA-1 ¹²

Boeing will continue to use SHA-1 for issuing end entity certificates after 12/31/2010. Boeing plans to move to SHA-256 when required by CertiPath.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA keys shall be generated in accordance with ANSI X9.31. Prime numbers for RSA shall be generated or tested for primality in accordance with ANSI X9.80.

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

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

The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* and *nonrepudiation* bits.

Certificates to be used for encryption shall set the *keyEncipherment* bit.

Certificates to be used for key agreement shall set the *keyAgreement* bit.

CA certificates shall set *cRLSign* and *CertSign* bits.

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates and require setting both *digitalsignature* and *keyEncipherment* bits to be set.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

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

Medium-hardware assurance tokens shall not output private keys in plaintext form.

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. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

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

For some purposes (such as data recovery), it will be necessary to provide key retrieval for the private component of the encryption certificate key pair. When encryption certificates are issued by the Boeing CA covered by this policy, the private key shall be escrowed. Boeing shall offer key escrow and recovery capability under the CertiPath Key Recovery Policy.

The method, procedures and controls which will apply to the storage, request for extraction and/or retrieval, delivery protection and destruction of the requested copy of an escrowed key shall be described in a Key Recovery Practice Statement that has been paired with the CertiPath Key Recovery Policy.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as the original signature key (see section 5.2.2). A single copy of the signature key may be kept at the CA location; a second copy may be kept at the CA backup location; a third copy may be kept at the DR location.

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

6.2.4.2 Backup of subscriber private signature key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the medium-software may be backed up or copied, but must be held in the Subscriber's control.

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

6.2.4.3 Backup of CSA Private Signature Key

"No stipulation until the Boeing CSA is implemented".

6.2.5 Private Key Archival

Private signature keys shall not be archived.

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys shall be generated by and remain in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary. CA and CMS private keys may be backed up in accordance with Section 6.2.4.

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

Subscriber private keys used for non-repudiation must be generated by and remain in a cryptographic module. Subscriber private keys used for encryption may be generated or escrowed outside of a cryptographic module in accordance with section 4.12 and 6.1.1.3.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store private keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-1/2 rating of the cryptographic module.

6.2.8 Method of Activating Private Keys

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

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

6.2.9 Methods of Deactivating Private Keys

Cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, (e.g., via a manual logout procedure or automatically after a period of inactivity) as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Keys

Private signature keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. For hardware cryptographic tokens, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods/Key Usage Periods

The validity period of a certificate must not exceed the lifetime of the key, as listed in Section 5.6.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock a CA, CMS, RA, or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Subscriber activation data may be user selected. For CAs, it shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module. If the activation data must be

transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

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

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

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

- Require authenticated logins
- Provide Discretionary Access Control, including managing privileges of users to limit users to their assigned roles
- Provide a security audit capability (See Section 5.4)
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Provide domain isolation for processes
- Provide self-protection for the operating system
- Require self-test security related CA services (e.g., check the integrity of the audit logs)
- Support recovery from key or system failure

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

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

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

The configuration of a CA, RA and CMS as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to a CA, RA and CMS software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of a CA, RA and CMS system. CA, RA and CMS software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to CA, CMS, and RA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the PKI equipment to those required to perform PKI functions.

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

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

6.8 TIME STAMPING

All CA components shall regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol (NTP) Service.

Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates

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

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

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

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

Issuer CA and Subscriber certificates may include any extensions as specified by RFC 3280 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.

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

7.1.3 Algorithm Object Identifiers

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

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
ecdsa-with-Sha1	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA1(1)}

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

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

7.1.4 Name Forms

The subject and issuer fields of the certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC3280. Subject and issuer fields shall include attributes as detailed in the table below.

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

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See right	0...1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Certification Authorities", or similar text

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

Table 1 Subject Name Forms (CA)

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

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as it appears in the CA certificate(s)

Table 2 Subject Name Form (Non-CA)

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

7.1.5 Name Constraints

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

The Issuer CA may obscure a Subscriber 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

CA and Subscriber Certificates issued under this CP shall assert one or more of the certificate policy OIDs listed in Section 1.2 of this document. When a CA asserts a policy OID, it shall also assert all lower assurance policy OIDs. Thus, for example:

1. If a CA issues a medium-software certificate it can also assert a medium-CBP-software policy OIDs. .
2. If a CA issues SHA-1 end entity certificates after 12/31/2010, the CA must only use "id-SHA1-....." certificate policy OIDs in the end entity certificates.

7.1.7 Usage of Policy Constraints Extension

The Boeing PCA shall adhere to the Certificate Formats described in this CP since inhibiting policy mapping may limit interoperability.

7.1.8 Policy Qualifiers Syntax & Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL PROFILE

7.2.1 Version Numbers

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

7.2.2 CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use.
Section 10 contains the CRL formats

7.3 OCSP PROFILE

No stipulation until Boeing OCSP is implemented

7.3.1 Version Number

No stipulation until Boeing OCSP is implemented

7.3.2 OCSP Extensions

No stipulation until Boeing OCSP is implemented

8. COMPLIANCE AUDIT & OTHER ASSESSMENTS

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

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

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

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

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either shall be a private firm, which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. The Boeing PA shall determine whether a compliance auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a component operates in accordance with the applicable CP, the component CPS, and the applicable governing agreements between Boeing, CertiPath and other Entities.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The Boeing PA may determine that a CA is not complying with its obligations set forth in this CP or the applicable governing agreements. When such a determination is made, the Boeing PA may suspend operation of a noncompliant CA it controls, or may direct the Boeing Operational Authority to cease interoperating with the affected CA (e.g., by revoking the cross or subordinate certificate issued to the CA), or may direct that other corrective actions be taken which allow interoperation to continue. If the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, the governing agreements, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Certification Authority of the discrepancy. The Certification Authority shall notify the Boeing PKI PA promptly;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP

and the governing agreement, and then proceed to make such notifications and take such actions without delay.

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

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the Certification Authority, shall be provided to the Boeing PA as set forth in Section 8.1. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

9. OTHER BUSINESS & LEGAL MATTERS

9.1 FEES

Not Applicable.

9.1.1 Certificate Issuance/Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fee

No Stipulation.

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

No Stipulation.

9.2 FINANCIAL RESPONSIBILITY

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

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information treated as Private

No stipulation.

9.4.3 Information not deemed Private

Information included in Boeing CA certificates is not subject to protections outlined in Section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to use Private Information

No Stipulation.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS & WARRANTIES

Boeing disclaims any liability that may arise from use of any certificate issued by the CA or from the PA's determination to revoke a certificate issued by the CA. In no event will Boeing be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the CA.

9.6.1 Certification Authority Representations and Warranties

Boeing certificates are issued and revoked at the sole discretion of the Boeing PKI Policy Authority. When the Boeing PCA issues a cross-certificate to a non-Boeing CA, it does so for the convenience of the Boeing Company.

Boeing Certification Authorities shall agree to the following:

- The Boeing CA's signing keys are protected and that no unauthorized person has ever had access to the private keys.
- All representations made by the Certification Authority in the applicable agreements are submitted are true and accurate, to the best knowledge of the Certification Authority.
- All information supplied by the Subscriber in connection with, and/or contained in the Certificate is true.
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this and any other applicable CP or CPS, to the best knowledge of the Certification Authority.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities and other subscribers.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their Subscriber Agreements, and local procedures.
- Notify, in a timely manner, the OA/PA of the CA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

9.6.4 Relying Parties Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.6.5 Representations and Warranties of other Participants

None.

9.7 *DISCLAIMERS OF WARRANTIES*

No stipulation.

9.8 *LIMITATIONS OF LIABILITY*

No stipulation.

9.9 INDEMNITIES

No stipulation.

9.10 TERM & TERMINATION

9.10.1 Term

No stipulation.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

None.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

None.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

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

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

9.12.2 Notification Mechanism and Period

Changes to the CP resulting from reviews and approval by the Boeing PKI PA are published online at <http://crl.boeing.com/crl/>. In addition, changes are communicated by the OA Manager to all cross-certified partners.

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

9.12.3 Circumstances under which OID must be changed

OIDs shall be changed if the Boeing PKI Policy Authority determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. CERTIFICATE, CRL AND OCSP FORMATS

This section contains the formats for the various PKI objects such as certificates and CRLs. The section only contains certificate profiles based on RSA. For algorithm identifiers, parameter encoding, public key encoding, and signature encoding for ECDSA and ECDH, RFC3279 shall be used.

Certificates and CRLs issued under a policy OID of this CP shall not contain any critical extensions not listed in the profiles in this section. Certificates and CRLs issued under a policy OID of this CP may contain non-critical extensions not listed in the profiles in this section only upon CPMA approval.

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

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

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

10.1 BOEING PCA TO CBCA CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Validity Period	Up to 12/31/2013 for SHA-1 Expressed in UTCTime until end of 2049 and Generalized Time for dates thereafter
Subject Distinguished Name	cn=CertiPath Bridge CA, ou=Certification Authorities, o=CertiPath LLC, c=us
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; SHA-1{1.3.6.1.4.1.73.15.3.1.4} {1.3.6.1.4.1.73.15.3.1.5} {1.3.6.1.4.1.73.15.3.1.8} {1.3.6.1.4.1.73.15.3.1.9}
Policy Mapping	c=no; [{1.3.6.1.4.1.73.15.3.1.4} {1.3.6.1.4.1.24019.1.1.1.17}] [{1.3.6.1.4.1.73.15.3.1.4} {1.3.6.1.4.1.24019.1.1.1.18}] [{1.3.6.1.4.1.73.15.3.1.4} {1.3.6.1.4.1.24019.1.1.1.19}] [{1.3.6.1.4.1.73.15.3.1.5} {1.3.6.1.4.1.24019.1.1.1.18}] [{1.3.6.1.4.1.73.15.3.1.5} {1.3.6.1.4.1.24019.1.1.1.19}]
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Directory Address: O=Boeing, C=US DNS Name: Boeing.com RFC822 Name: Boeing.com RFC822 Name: .Boeing.com
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository.</i>

Field	Value
CRL Distribution Points ¹³	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.”</i>
Inhibit anyPolicy	c=no; skipCerts = 0

10.2 BOEING PCA SELF-SIGNED ROOT CERTIFICATE (ALSO CALLED TRUST ANCHOR)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Validity Period	20 years from date of issue Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Subject Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; cA=True; path length constraint absent

¹³ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.3 INTERMEDIATE OR SIGNING CA CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Validity Period	10 years from date of issue, but not beyond the validity period of its parent CA Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; SHA-1{1.3.6.1.4.1.73.15.3.1.4} and {1.3.6.1.4.1.73.15.3.1.5} {1.3.6.1.4.1.73.15.3.1.10}
Basic Constraints	c=yes; cA=True; path length=0
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository.</i>
CRL Distribution Points ¹⁴	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.”</i>

¹⁴ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.4 MEDIUM HARDWARE SUBSCRIBER IDENTITY CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=<first>.<mi>.<last>.<bemsid>, OU=People, O=Boeing, C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
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)
Key Usage	c=yes; digitalSignature; nonRepudiation
Extended Key Usage	c=no, Client Authentication {1.3.6.1.5.5.7.3.2}, Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.5}
Subject Alternative Name	c=no; Principal Name = Windows UPN URI ¹⁵ : urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ¹⁶	c = no; The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."

¹⁵ Note this name form is tagged [6] and encoded as IA5String.

¹⁶ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL

10.5 MEDIUM SOFTWARE SUBSCRIBER IDENTITY CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=<first>.<mi>.<last>.<bemsid>, OU=People, O=Boeing, C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
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)
Key Usage	c=yes; digitalSignature; nonRepudiation
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.4}
Extended Key Usage	C=no, Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	c=no; Principal Name = Windows UPN
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ¹⁷	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."</i>

that does NOT contain the issuer distribution point extension).

¹⁷ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons

10.6 MEDIUM HARDWARE SUBSCRIBER SIGNATURE CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=Boeing SecureBadge Med Hardware <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=<first>.<mi>.<last>.<bemsid>, OU=People, O=Boeing, C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	critical no Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.5}
Subject Alternative Name	c=no; RFC822 email address ; URI ¹⁸ : urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>

and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

¹⁸ Note this name form is tagged [6] and encoded as IA5String.

Field	Value
CRL Distribution Points ¹⁹	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.”</i>

¹⁹ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.7 MEDIUM SOFTWARE SUBSCRIBER SIGNATURE CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN=<first>.<mi>.<last>.<bemsid>, OU=People, O=Boeing, C=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	critical no Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.4}
Subject Alternative Name	c=no; RFC822 email address

Field	Value
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ²⁰	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."</i>

10.8 MEDIUM HARDWARE SUBSCRIBER ENCRYPTION CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, =Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} }
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment

²⁰ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

Field	Value
Extended Key Usage	critical no Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies ²¹	c=no; {1.3.6.1.4.1.73.15.3.1.5}
Subject Alternative Name	c=no; RFC822 email address, URI ²² : urn:uuid:<32 hex representing 128 bit GUID> (optional) others optional
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ²³	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."</i>

²² Note this name form is tagged [6] and encoded as IA5String.

²³ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.9 MEDIUM SOFTWARE SUBSCRIBER ENCRYPTION CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment
Extended Key Usage	critical no Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies ²⁴	c=no; {1.3.6.1.4.1.73.15.3.1.4}
Subject Alternative Name	c=no; RFC822 email address (required)
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ²⁵	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.</i>

²⁴

²⁵ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.10 CODE SIGNING CERTIFICATE – PLACE HOLDER ONLY

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
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}
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)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3) }
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.5}
Subject Alternative Name	DN of the person controlling the code signing private key
CRL Distribution Points ²⁶	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA;

²⁶ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.11 MEDIUM HARDWARE DEVICE OR SERVER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL Host IP Address Host Name }
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}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	c=no; Server Authentication {1.3.6.1.5.5.7.3.1}; Client Authentication {1.3.6.5.5.7.3.2} or both
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.5}
Subject Alternative Name	c=no; always present, Host URL IP Address Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA;
CRL Distribution Points ²⁷	c = no; always present

²⁷ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.12 MEDIUM SOFTWARE DEVICE OR SERVER CERTIFICATE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN=Boeing SecureBadge Med Hardware <n>, OU=Certservers, O=Boeing, C=US
Validity Period	3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL Host IP Address Host Name }
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}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	c=no; Server Authentication {1.3.6.1.5.5.7.3.1}; Client Authentication {1.3.6.5.5.7.3.2} or both
Certificate Policies	c=no; {1.3.6.1.4.1.73.15.3.1.4}
Subject Alternative Name	c=no; always present, Host URL IP Address Host Name
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA;
CRL Distribution Points ²⁸	c = no; always present

²⁸ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

10.13 OCSP RESPONDER CERTIFICATE – PLACE HOLDER ENTRY ONLY

The following table contains the OCSP Responder certificate profile assuming that the OCSP Responder certificate is signed by the same CA using the same private key as the Subscriber Certificate. Alternative trust models shall not be supported by this policy.

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	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
Validity Period	No longer than one month from date of issue expressed in UTCTime until 2030
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
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)
Key Usage	C=yes; nonRepudiation, digitalSignature
Extended key usage	C=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies ²⁹	c=no; {1.3.6.1.4.1.73.15.3.1.5} {1.3.6.1.4.1.73.15.3.1.4}
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	C=no; Null

²⁹ Technically the Responder certificate need not have a CP OID in it; but, not everyone and every product gets the Gestalt behind PKI. Thus, we include this extension to help product interoperability.

Field	Value
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to issuing CA or LDAP URL pointer to the caCertificate attribute of the Issuing CA

10.14 CRL FORMAT

Full and Complete CRL

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

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP Example CN=Boeing PCA Med Hardware,<n>, OU=Certservers, 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 UTCTime)
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
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

10.15 OCSP REQUEST FORMAT – PLACE HOLDER ONLY

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	Value
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	Value
None	None
Request Entry Extension	Value
None	None

10.16 OCSP RESPONSE FORMAT – PLACE HOLDER ONLY

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response shall contain certificate id; certificate status ³⁰ , thisUpdate, nextUpdate ³¹ ,
Responder Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	Value
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	Value
None	None

³⁰ If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.

³¹ The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

10.17 MEDIUM ASSURANCE RA ENROLLMENT AGENT CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN=Boeing SecureBadge Medium G2 <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP Example: CN = AEASVC01,OU = Service Accounts,OU = SSG,OU = Bellevue,OU = Accounts,DC = nw,DC = nos,DC = boeing,DC = com
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=no; digitalSignature (always present), nonRepudiation (optional)
Enhanced Key Usage	C=no; Certificate Request Agent (1.3.6.1.4.1.311.20.2.1)
Certificate Template Information	Template=1.3.6.1.4.1.311.21.8.4456910.5413282.8343170.10132414.1783414.214.5792733.2512321 Major Version Number=100 Minor Version Number=8
Certificate Template Name:	Enrollment Agent
Application Policy	[1]Application Certificate Policy: Policy Identifier=Certificate Request Agent
Basic Constraints:	Subject Type=End Entity, Path Length Constraint=None
Subject Alternative Name	c=no; Principal Name = Windows UPN

Field	Value
Authority Information Access	c=no; The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository
CRL Distribution Points ³²	c = no; The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.”

³² The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.18 MEDIUM ASSURANCE QUALIFIED SUBORDINATION CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN=Boeing PCA Med Hardware <n>, OU=Certservers, O=Boeing, C=US
Validity Period	No longer than 6 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Enhanced Key Usage	C=no; Certificate Request Agent (1.3.6.1.4.1.311.20.2.1)
Authority Information Access	c=no; <i>The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository</i>
CRL Distribution Points ³³	c = no; <i>The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."</i>

³³ The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain LDAP (i.e., of the form ldap://...) and/or HTTP (i.e., of the form http://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.19 MEDIUM ASSURANCE CA EXCHANGE CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN = Boeing SecureBadge Medium G2 OU = certservers O = Boeing C = US
Validity Period	No longer than 7 days from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	CN = Boeing SecureBadge Medium G2-Xchg OU = certservers O = Boeing C = US
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; Key Encipherment (20)
Enhanced Key Usage	Private Key Archival (1.3.6.1.4.1.311.21.5)
Certificate Policies	C=?; [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.4 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.5 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.10
Authority Information Access	c=no; The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository

Field	Value
CRL Distribution Points	c = no; The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository.”
Certificate Template Name	CAExchange
Certificate Template Information	Template=1.3.6.1.4.1.311.21.8.3108027.7675824.6176946.5856084.1236705.27.1.26 Major Version Number=106 Minor Version Number=0
Application Policies	[1]Application Certificate Policy: Policy Identifier=Private Key Archival

10.20 MEDIUM ASSURANCE KEY RECOVERY AGENT (KRA) CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN = Boeing SecureBadge Medium G2 OU = certservers O = Boeing C = US
Validity Period	No longer than 3 years days from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	CN = MAHKeyRecAgent
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; Key Encipherment (20)
Enhanced Key Usage	Key Recovery Agent (1.3.6.1.4.1.311.21.6)
Certificate Policies	C=?; [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.4 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.5 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.10
Authority Information Access	c=no; The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository
CRL Distribution Points	c = no; The CRL Distribution points will be referenced by HTTP and/or LDAP URLs referencing a Boeing public PKI repository."

Field	Value
Certificate Template Name	
Certificate Template Information	Template=1.3.6.1.4.1.311.21.8.4456910.5413282.8343170.10132414.178 3414.214.12212852.10596623 Major Version Number=100 Minor Version Number=7
Application Policies	[1]Application Certificate Policy: Policy Identifier=Key Recovery Agent

10.21 MEDIUM ASSURANCE CARD AUTHENTICATION CERTIFICATE PROFILE

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	CN = Boeing SecureBadge Medium G2 OU = certservers O = Boeing C = US
Validity Period	No longer than 3 years from date of issue expressed in UTCTime
Subject Distinguished Name	CN = SecureBadge OU = certservers O = Boeing C = US
Subject Public Key Information	2048 bit RSA key modulus or greater, rsaEncryption
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	Value
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	
Enhanced Key Usage	
Certificate Policies	C=?; [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.73.15.3.1.10
Authority Information Access	c=no; The Certificate Authority Issuer certificate will be specified by an HTTP URL referencing a Boeing public PKI repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.boeing.com/crl/Boeing%20SecureBadge%20Medium%20G2.crl URL=ldap://dir.boeing.com/CN=Boeing%20SecureBadge%20Medium%20G2,ou=pki,ou=certservers,o=boeing,c=us?certificateRevocationList;binary

11. PROTOCOL

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

- Protocol
- Authentication
- Naming
- Object Class
- Attributes

Each of these items is described below.

11.1 PROTOCOL

Boeing PKI Repositories shall provide HTTP and LDAP protocol access to certificates and CRLs.

11.2 AUTHENTICATION

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

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

11.3 NAMING

This CP has defined the naming convention. Certificates shall be stored in the PKI Repository in the entry that appears in the certificate subject name. issuedByThisCA element of crossCertificatePair shall contain the certificate(s) issued by a CA whose name the entry represents.

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

11.4 OBJECT CLASS

Entries that describe CAs shall be defined by organizationUnit structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes.

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

11.5 ATTRIBUTES

CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cpCPS attributes, as applicable.

User entries shall be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the PKI Repository.

12. ACRONYMS & ABBREVIATIONS

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

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union—Telecommunications Sector
ITU-TSS	International Telecommunications Union—Telecommunications System Sector
NIST	National Institute of Standards and Technology
NSA	National Security Entity
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
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
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

13. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [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 subscriber is sometimes also called an "applicant" after applying to the Certification Authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the Boeing PKI PA body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [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]
Biometric	A physical or behavioral characteristic of a human being.

Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list of the certificates maintained by a CA which it has issued and that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Entity as defined above.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End-entity	Relying Parties and Subscribers.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.
Boeing Operational Authority (Boeing OA)	The Boeing Public Key Infrastructure Operational Authority is the organization selected by the Boeing I Public Key Infrastructure Policy Authority to be responsible for operating the Boeing Certification Authority.
Boeing Public Key Infrastructure Policy Authority (PA)	The PA is a Boeing body responsible for setting, implementing, and administering policy decisions regarding interEntity PKI interoperability that uses the Boeing Principal CA or its Subordinate CAs.
Firewall	Gateway that limits access between networks in accordance with local security policy. [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.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
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.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the Boeing PA and any Entity allowing interoperability between the Boeing Principal CA and an Entity CA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
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.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the another Entity CA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.

Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
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. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
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/dsqfree.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.
- OCSF
- 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

This Certificate Policy was re-formatted from RFC 2527 to RFC 3647 for submission to CertiPath.