Lockheed Martin
Enterprise Public Key Infrastructure
Certificate Policy (CP)

Version 10.1

August 2025

Copyright, Lockheed Martin, 2025

Questions or comments regarding the Lockheed Martin PKI Certification Practice Statement or this Certificate Policy should be communicated to the PKI point of contact specified in section 1.5.2 of this document.

Document Change History

LM PKI Certificate Policy

VER	DATE	INFORMATION AFFECTED	RFC	AUTHORIZED BY
1.0	12/20/00	Baselined	--	PKI Team
2.0	5/21/2003		--	PKI Team
3.0	9/22/2003	Updated to include Key Recovery Policy information and Certificate Policy Information	--	PKI Team
4.0	10/10/05	New Policy written to support CertiPath Medium Assurance	--	LM PMA
	04/2006	Updates based on KPMG audit observations	--	PKI Team
5.0	8/29/2006	Minor updates based on KPMG observations and addition of Name Constraints to PCA -> CBCA certificate profile	--	LM PMA
6.0	7/16/2007	Minor updates based upon KPMG annual operational audit results	--	LM PMA
7.0	December 2007	Updates based upon Slalom Consulting audit	--	LM PMA
7.0	May 2008	Updated to include Assured Identity requirements	--	LM PMA
7.1	June 2008	Update based on delta compliance audit	--	LM PMA
8.0	February 2010	Updates based on annual compliance audit and Assured Identity release 2.1.1 requirements	--	LM PMA
8.1	January 2011	Updates to section 6.1.5 related to SHA-256 support	--	LM PMA
8.2	February 2011	Updates to sections 3.2.3.2 and 3.2.3.3.	--	LM PMA

LM PKI Certificate Policy

VER	DATE	INFORMATION AFFECTED	RFC	AUTHORIZED BY
8.3 Draft	October 2011	Updates to sections 1.3.6, 1.5.2, 3.3.1, 4.9.7, 6.1.5, 10 and 10.8	--	LM PMA
8.4	April 2012	Updates to sections 1.2, 2.2.1, 3.2.3.1, 5.3.2, 6.1.5, 7.1.6, and 8.4 to improve alignment with CertiPath's recent CP revisions; and minor grammatical changes throughout which add clarity to the existing requirements. Updates made to Bibliography to add references and to correct broken hyperlinks.	--	LM PMA
8.5	November 2012	Updates to improve alignment with CertiPath's CP, incorporating many of their 2012 revisions.	--	LM PMA
8.6	August 2013	Updates to improve alignment with CertiPath's CP, incorporating many of their 2013 revisions.	--	LM PMA
8.7	April 2014	Updates to improve alignment with CertiPath's CP, incorporating many of their later-2013 revisions.	--	LM PMA
8.8	April 2015	Changes to numerous sections to support policy updates to the LM CP which were brought about due to the establishment of a new Bridge relationship with TSCP.	--	LM PMA
8.9	January 2016	Changes to Sections 7, 9 and 10, in support of the cross-certification of LM's PKI with the TSCP Commercial Bridge Authority.	--	LM PMA
8.10	April 2016	Updates to improve alignment with CertiPath's CP.	--	LM PMA
8.11	January 2017	Updates to improve alignment with CertiPath's CP.	--	LM PMA

LM PKI Certificate Policy

VER	DATE	INFORMATION AFFECTED	RFC	AUTHORIZED BY
8.12	May 2017	Updates to Sections 1.2, 6.4.1 and 10 to improve alignment with CertiPath's CP.	--	LM PMA
8.13	Feb 2018	Updates to Sections 1.3.1.1, 4.4.3, 4.9, 5.7.1, 5.7.2, 5.7.3, 5.8 and 9.11 to align with recent changes to the FBCA CP flowing down through CertiPath's CP to this CP.	--	LM PMA
8.14	March 2019	Updates to Sections 1.2, 3.2.3, 4.10.2, 6.1.5, 6.2.8, 7.1.4, 7.1.5, 9.4, 10.12 and 10.13 to align with recent changes to the FBCA CP flowing down through CertiPath's CP to this CP. Added Microsoft-proprietary extension to Section 10.	--	LM PMA
8.15	February 2020	Updates to improve alignment with CertiPath's CP.	--	LM PMA
8.16	March 2020	Updates to improve alignment with CertiPath's CP and removal of all SHA-1 specific policies within the document.	--	(internal version, unpublished)
8.17	March 2021	Further updates to improve alignment with CertiPath's CP.	--	LM PMA
8.18	February 2022	Minor edits to various acronyms & informational sections for synchronicity with CertiPath's CP.	--	LM PMA
8.19	July 2022	Edits to Certificate Profiles to include Generation 3 (G3) CA naming conventions & various related errata changes to support addition of G3 CAs.	--	LM PMA

LM PKI Certificate Policy

VER	DATE	INFORMATION AFFECTED	RFC	AUTHORIZED BY
9.0	February 2024	Updates to improve alignment with CertiPath's CP (as recently revised.) Corrections in Section 10 w/r/t the DN of LM's 4096-bit Root CA ('Root CA 6')	--	LM PMA
9.1	April 2024	Minor revisions needed to keep LM's CP document in alignment with CertiPath's CP.	--	LM PMA
10.0	March 2025	Updates to improve alignment with CertiPath's CP v4 (as recently revised) which incorporated all requirements related to Key Escrow and Key Recovery (formerly a separate policy document) into the body of this document.	--	LM PMA
10.1	August 2025	Updates to improve alignment with CertiPath's June 2025 revisions to their CP v4	--	LM PMA

Contact Information

Organization: Corporate Information Security
Please reference section 1.5.2 for the current contact point information.

Table of Contents

1 INTRODUCTION 12

1.1 OVERVIEW 12
1.1.1 Certificate Policy (CP) 12
1.1.2 Relationship between this CP & the LM Certification Practice Statement (CertPS) 13
1.1.3 Scope 13
1.2 DOCUMENT IDENTIFICATION 14
1.3 PKI PARTICIPANTS 15
1.3.1 PKI Authorities 15
1.3.2 Registration Authority (RA) 19
1.3.3 Certificate Holder 20
1.3.4 Relying Parties 21
1.3.5 Other Participants 21
1.3.6 Applicability 22
1.4 CERTIFICATE USAGE 23
1.4.1 Appropriate Certificate Uses 23
1.4.2 Prohibited Certificate Uses 23
1.5 POLICY ADMINISTRATION 23
1.5.1 Organization administering the document 23
1.5.2 Contact Point 23
1.5.3 Person Determining Certification Practice Statement Suitability for the Policy 23
1.5.4 Certification Practice Statement (CertPS) Approval Procedures 23
1.5.5 Waivers 24

2 PUBLICATION & PKI REPOSITORY RESPONSIBILITIES 25

2.1 PKI REPOSITORIES 25
2.2 PUBLICATION OF CERTIFICATE INFORMATION 25
2.2.1 Publication of CA Information 25
2.2.2 Certificate Policy Publication 26
2.3 TIME OR FREQUENCY OF PUBLICATION 26
2.4 ACCESS CONTROLS ON REPOSITORIES 26

3 IDENTIFICATION & AUTHENTICATION 27

3.1 NAMING 27
3.1.1 Types of Names 27
3.1.2 Need for Names to be Meaningful 27
3.1.3 Anonymity or Pseudonymity of Certificate holders 27
3.1.4 Rules for Interpreting Various Name Forms 28
3.1.5 Uniqueness of Names 28
3.1.6 Recognition, Authentication & Role of Trademarks 28
3.1.7 Name Claim Dispute Resolution Procedure 28
3.2 INITIAL IDENTITY VALIDATION 28
3.2.1 Method to Prove Possession of Private Key 28
3.2.2 Authentication of Organization Identity 29
3.2.3 Authentication of Individual Identity 29
3.2.4 Non-verified Certificate holder Information 32
3.2.5 Validation of Authority 32
3.2.6 Criteria for Interoperation 33
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 33
3.3.1 Identification and Authentication for Routine Re-key 33
3.3.2 Identification and Authentication for Re-key after Revocation 34
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 34

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 35

4.1 CERTIFICATE APPLICATION 35
4.1.1 Submission of Certificate Application 36
4.1.2 Enrollment Process and Responsibilities 36
4.2 CERTIFICATE APPLICATION PROCESSING 37
4.2.1 Performing Identification and Authentication Functions 37
4.2.2 Approval or Rejection of Certificate Applications 37
4.2.3 Time to Process Certificate Applications 38
4.3 CERTIFICATE ISSUANCE 38
4.3.1 CA Actions during Certificate Issuance 38
4.3.2 Notification to Certificate holder of Certificate Issuance 38
4.4 CERTIFICATE ACCEPTANCE 38
4.4.1 Conduct Constituting Certificate Acceptance 39
4.4.2 Publication of the Certificate by the CA 39
4.4.3 Notification of Certificate Issuance by the CA to Other entities 39
4.5 KEY PAIR AND CERTIFICATE USAGE 39
4.5.1 Certificate holder Private Key and Certificate Usage 39
4.5.2 Relying Party Public Key and Certificate Usage 40
4.6 CERTIFICATE RENEWAL 40
4.6.1 Circumstance for Certificate Renewal 40
4.6.2 Who may Request Renewal 40
4.6.3 Processing Certificate Renewal Requests 40
4.6.4 Notification of New Certificate Issuance to Certificate holder 41
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 41
4.6.6 Publication of the Renewal Certificate by the CA 41
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 41
4.7 CERTIFICATE RE-KEY 41
4.7.1 Circumstance for Certificate Re-key 41
4.7.2 Who may Request Certification of a New Public Key 41
4.7.3 Processing Certificate Re-keying Requests 41
4.7.4 Notification of New Certificate Issuance to Certificate holder 42
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 42
4.7.6 Publication of the Re-keyed Certificate by the CA 42
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 42
4.8 CERTIFICATE MODIFICATION 42
4.8.1 Circumstance for Certificate Modification 42
4.8.2 Who may Request Certificate Modification 42
4.8.3 Processing Certificate Modification Requests 42
4.8.4 Notification of New Certificate Issuance to Certificate holder 42
4.8.5 Conduct Constituting Acceptance of Modified Certificate 43
4.8.6 Publication of the Modified Certificate by the CA 43
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 43
4.9 CERTIFICATE REVOCATION AND SUSPENSION 43
4.9.1 Circumstance for Revocation of a Certificate 43
4.9.2 Who Can Request Revocation of a Certificate 43
4.9.3 Procedure for Revocation Request 44
4.9.4 Revocation Request Grace Period 44
4.9.5 Time within which CA must Process the Revocation Request 44
4.9.6 Revocation Checking Requirements for Relying Parties 45
4.9.7 CRL Issuance Frequency 45
4.9.8 Maximum Latency for CRLs 46
4.9.9 Online Revocation Checking Availability 46
4.9.10 Online Revocation Checking Requirements 46
4.9.11 Other Forms of Revocation Advertisements Available 46
4.9.12 Special Requirements Related To Key Compromise 46

4.9.13 Circumstances for Suspension *46*
4.9.14 Who can Request Suspension *46*
4.9.15 Procedure for Suspension Request *47*
4.9.16 Limits on Suspension Period *47*
4.10 CERTIFICATE STATUS SERVICES 47
4.10.1 Operational Characteristics *47*
4.10.2 Service Availability *47*
4.10.3 Optional Features *47*
4.11 END OF SUBSCRIPTION 47
4.12 KEY ESCROW AND RECOVERY 47
4.12.1 Key Escrow and Recovery Policy and Practices *47*
4.12.2 Session Key Encapsulation and Recovery Policy and Practices *53*

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS 54

5.1 PHYSICAL CONTROLS 54
5.1.1 Site Location & Construction *54*
5.1.2 Physical Access *54*
5.1.3 Power and Air Conditioning *55*
5.1.4 Water Exposures *55*
5.1.5 Fire Prevention & Protection *55*
5.1.6 Media Storage *56*
5.1.7 Waste Disposal *56*
5.1.8 Off-Site backup *56*
5.2 PROCEDURAL CONTROLS 56
5.2.1 Trusted Roles *56*
5.2.2 Number of Persons Required per Task *58*
5.2.3 Identification and Authentication for Each Role *59*
5.2.4 Roles Requiring Separation of Duties *59*
5.3 PERSONNEL CONTROLS 59
5.3.1 Qualifications, Experience, and Clearance Requirements *59*
5.3.2 Background Check Procedures *60*
5.3.3 Training Requirements *61*
5.3.4 Retraining Frequency and Requirements *61*
5.3.5 Job Rotation Frequency and Sequence *62*
5.3.6 Sanctions for Unauthorized Actions *62*
5.3.7 Independent Contractor Requirements *62*
5.3.8 Documentation Supplied To Personnel *62*
5.4 AUDIT LOGGING PROCEDURES 62
5.4.1 Types of Events Recorded *63*
5.4.2 Frequency of Processing Audit Logs *68*
5.4.3 Retention Period for Audit Logs *68*
5.4.4 Protection of Audit Logs *68*
5.4.5 Audit Log Backup Procedures *68*
5.4.6 Audit Collection System (internal vs. external) *68*
5.4.7 Notification to Event-Causing Subject *69*
5.4.8 Vulnerability Assessments *69*
5.5 RECORDS ARCHIVAL 69
5.5.1 Types of Records Archived *69*
5.5.2 Retention Period for Archive *70*
5.5.3 Protection of Archive *70*
5.5.4 Archive Backup Procedures *71*
5.5.5 Requirements for Time-Stamping of Records *71*
5.5.6 Archive Collection System (internal or external) *71*
5.5.7 Procedures to Obtain & Verify Archive Information *71*
5.6 KEY CHANGEOVER 71
5.7 COMPROMISE AND DISASTER RECOVERY 72

5.7.1 Incident and Compromise Handling Procedures *72*
5.7.2 Computing Resources, Software, and/or Data Corruption *73*
5.7.3 Private Key Compromise Procedures *73*
5.7.4 Business Continuity Capabilities after a Disaster *75*
5.8 CA, CSA, KED, DDS AND RA TERMINATION 75

6 TECHNICAL SECURITY CONTROLS 75

6.1 KEY PAIR GENERATION AND INSTALLATION 75
6.1.1 Key Pair Generation *75*
6.1.2 Private Key Delivery to Certificate holder *76*
6.1.3 Public Key Delivery to Certificate Issuer *77*
6.1.4 CA Public Key Delivery to Relying Parties *77*
6.1.5 Key Sizes *77*
6.1.6 Public Key Parameters Generation and Quality Checking *79*
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) *79*
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 79
6.2.1 Cryptographic Module Standards and Controls *79*
6.2.2 Private Key Multi-Person Control *80*
6.2.3 Private Key Escrow *80*
6.2.4 Private Key Backup *80*
6.2.5 Private Key Archival *81*
6.2.6 Private Key Transfer into or from a Cryptographic Module *81*
6.2.7 Private Key Storage on Cryptographic Module *81*
6.2.8 Method of Activating Private Key *81*
6.2.9 Methods of Deactivating Private Key *82*
6.2.10 Method of Destroying Private Key *82*
6.2.11 Cryptographic Module Rating *82*
6.3 OTHER ASPECTS OF KEY MANAGEMENT 82
6.3.1 Public Key Archival *82*
6.3.2 Certificate Operational Periods/Key Usage Periods *82*
6.4 ACTIVATION DATA 82
6.4.1 Activation Data Generation and Installation *82*
6.4.2 Activation Data Protection *83*
6.4.3 Other Aspects of Activation Data *83*
6.5 COMPUTER SECURITY CONTROLS 83
6.5.1 Specific Computer Security Technical Requirements *83*
6.5.2 Computer Security Rating *84*
6.6 LIFE-CYCLE TECHNICAL CONTROLS 84
6.6.1 System Development Controls *84*
6.6.2 Security Management Controls *85*
6.6.3 Life Cycle Security Controls *85*
6.7 NETWORK SECURITY CONTROLS 85
6.8 TIME STAMPING 86

7 CERTIFICATE, CRL, AND OCSP PROFILES 87

7.1 CERTIFICATE PROFILE 87
7.1.1 Version Numbers *87*
7.1.2 Certificate Extensions *87*
7.1.3 Algorithm Object Identifiers *87*
7.1.4 Name Forms *87*
7.1.5 Name Constraints *89*
7.1.6 Certificate Policy Object Identifier *89*
7.1.7 Usage of Policy Constraints Extension *89*
7.1.8 Policy Qualifiers Syntax and Semantics *89*
7.1.9 Processing Semantics for the Critical Certificate Policy Extension *89*
7.1.10 Inhibit Any Policy Extension *89*

7.2 CRL PROFILE 89
7.2.1 Version Numbers *89*
7.2.2 CRL and CRL Entry Extensions *90*
7.3 OCSP PROFILE 90
7.3.1 Version Number *90*
7.3.2 OCSP Extensions *90*

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 91

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS 91
8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR 91
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 91
8.4 TOPICS COVERED BY ASSESSMENT 91
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 92
8.6 COMMUNICATION OF RESULTS 92

9 OTHER BUSINESS AND LEGAL MATTERS 93

9.1 FEES 93
9.1.1 Certificate Issuance and Renewal Fees *93*
9.1.2 Certificate Access Fees *93*
9.1.3 Revocation or Status Information Access Fees *93*
9.1.4 Fees for Other Services *93*
9.1.5 Refund Policy *93*
9.2 FINANCIAL RESPONSIBILITY 93
9.2.1 Insurance Coverage *93*
9.2.2 Other Assets *93*
9.2.3 Insurance or Warranty Coverage for Relying Parties *93*
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 94
9.4 PRIVACY OF PERSONAL INFORMATION/PERSONAL DATA 94
9.5 INTELLECTUAL PROPERTY RIGHTS 94
9.5.1 Property Rights in Certificates and Revocation Information *94*
9.5.2 Property Rights in the CertPS *94*
9.5.3 Property Rights in Names *94*
9.5.4 Property Rights in Keys *94*
9.6 REPRESENTATIONS AND WARRANTIES 95
9.6.1 CA Representations and Warranties *95*
9.6.2 RA, KRA and KRO Representations and Warranties *95*
9.6.3 Certificate Holder *96*
9.6.4 Relying Party *97*
9.6.5 Representations and Warranties of Affiliated Organizations *97*
9.6.6 Representations and Warranties of Other Participants *97*
9.7 DISCLAIMERS OF WARRANTIES 98
9.8 LIMITATIONS OF LIABILITIES 99
9.9 INDEMNITIES 99
9.9.1 Indemnification by cross-certified CAs *99*
9.9.2 Indemnification by Relying Parties *100*
9.10 TERM AND TERMINATION 100
9.10.1 Term *100*
9.10.2 Termination *100*
9.10.3 Effect of Termination and Survival *101*
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 101
9.12 AMENDMENTS 101
9.12.1 Procedure for Amendment *101*
9.12.2 Notification Mechanism and Period *101*
9.12.3 Circumstances under Which OID Must be Changed *102*
9.13 DISPUTE RESOLUTION PROVISIONS 102
9.13.1 Disputes among Lockheed Martin and Customers *102*

9.13.2 Alternate Dispute Resolution Provisions *102*
9.14 GOVERNING LAW 103
9.15 COMPLIANCE WITH APPLICABLE LAW 103
9.16 MISCELLANEOUS PROVISIONS 103
9.16.1 Entire Agreement *103*
9.16.2 Assignment *103*
9.16.3 Severability *103*
9.16.4 Waiver of Rights *103*
9.16.5 Force Majeure *103*
9.17 OTHER PROVISIONS 104

10 CERTIFICATE, CRL, AND OCSP FORMATS 105

10.1 CROSS-CERTIFICATE FROM LM SIGNING CA TO COMMERCIAL BRIDGE CERTIFICATION AUTHORITY (CBCA) 106
10.2 LOCKHEED MARTIN OFF-LINE ROOT CA (ALSO CALLED TRUST ANCHOR) 109
10.3 INTERMEDIATE OR SIGNING CA CERTIFICATE 110
10.4 CERTIFICATE HOLDER CERTIFICATES – MEDIUM LEVEL OF ASSURANCE 112
10.4.1 Certificate holder Identity Certificate – Medium Software *113*
10.4.2 Certificate holder Identity Certificate – Medium Hardware *114*
10.4.3 Certificate holder Signature Certificate – Medium Software *115*
10.4.4 Certificate holder Signature Certificate – Medium Hardware *116*
10.4.5 Certificate holder Encryption Certificate – Medium Software *117*
10.4.6 Certificate holder Encryption Certificate – Medium Hardware *118*
10.5 CODE SIGNING CERTIFICATE 119
10.6 DEVICE OR SERVER CERTIFICATE 120
10.7 OCSP RESPONDER CERTIFICATE 121
10.8 PKCS 10 REQUEST FORMAT 121
10.9 CRL FORMAT 123
10.9.1 Full and Complete CRL *123*
10.9.2 Distribution Point Based Partitioned CRL *124*
10.9.3 Delta CRL *125*
10.10 OCSP REQUEST FORMAT 126
10.11 OCSP RESPONSE FORMAT 127
10.12 EXTENDED KEY USAGE 128
10.13 SUBJECT PUBLIC KEY INFORMATION FORMAT 130
10.14 LOCKHEED MARTIN INTERNAL CERTIFICATE TEMPLATES 130

11 PKI REPOSITORY INTEROPERABILITY PROFILE 131

11.1 PROTOCOL 131
11.2 AUTHENTICATION 131
11.3 NAMING 131
11.4 OBJECT CLASS 131
11.5 ATTRIBUTES 132

12 BIBLIOGRAPHY 133

13 ACRONYMS & ABBREVIATIONS 135

14 GLOSSARY 138

1 INTRODUCTION

The Lockheed Martin Enterprise Public Key Infrastructure (PKI) Certificate Policy (CP) defines five certificate policies to facilitate interoperability among distinct Aerospace industry Public Key Infrastructure domains. The five policies are all variants of the medium level of assurance issuance policy for public key certificates. Please refer to section 1.2 of this document for details on the five policies. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the certificate holder performs its task.

This CP incorporates the requirements for the escrow and key recovery of private decryption key management keys. In turn, key recovery practices are incorporated into the appropriate Certification Practice Statement (CertPS).

This CP is consistent with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Request for Comments (RFC) 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework, http://www.ietf.org/rfc/rfc3647.txt.

1.1 Overview

1.1.1 Certificate Policy (CP)

Certificates contain one or more registered **certificate policy object identifiers (OID),** which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. Each OID corresponds to a specific level of assurance established by this Certificate Policy (CP), which shall be available to Relying Parties. Certificates issued by the Lockheed Martin Certification Authority shall, in the *policyMappings* extension and in whatever other fashion is determined by the Lockheed Martin Policy Management 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's CP.

The key recovery requirements included in this CP are based on the principle that all encryption activities using the certificates are performed on behalf of Lockheed Martin, as Lockheed Martin authorized the issuance of encryption certificates. Therefore, Lockheed Martin has the right to identify the persons authorized to recover the decryption private key in order to maintain the continuity of business operations. In addition, Lockheed Martin may choose to require that the contents of incoming and/or outgoing encrypted email be examined for compliance with the organization's policies. Furthermore, there may be a need to access the information for investigative and law enforcement purposes.

1.1.2 Relationship between this CP & the LM Certification Practice Statement (CertPS)

This CP states what assurance can be placed in a certificate issued by the Lockheed Martin Certification Authority (CA). The Lockheed Martin CertPS states how the Lockheed Martin CA establishes that assurance.

Lockheed Martin uses the CPS acronym (used by the industry to mean Certification Practice Statement) to mean Corporate Policy Statement. To avoid confusion when referring to Certification Practice Statements within LM documents, the acronym will be CertPS.

1.1.3 Scope

The following diagram represents the scope of the LM CP. The LM Medium Level of Assurance Root and/or Signing CA shall cross-certify with the CertiPath and/or TSCP (or other LM PMA-Approved Bridge Authority's) Commercial Bridge Certification Authority (CBCA) which are in turn cross-certified with either a Federal or DoD Bridge Authority. Certificates for end entities, such as LM employees, are issued from the LM Medium Level of Assurance Signing CAs. The LM Medium Level of Assurance Signing CAs are subordinate to the LM Off-line Root CAs. Lockheed Martin has also established several identity management functions that will be employed to request, issue, and maintain certificates.

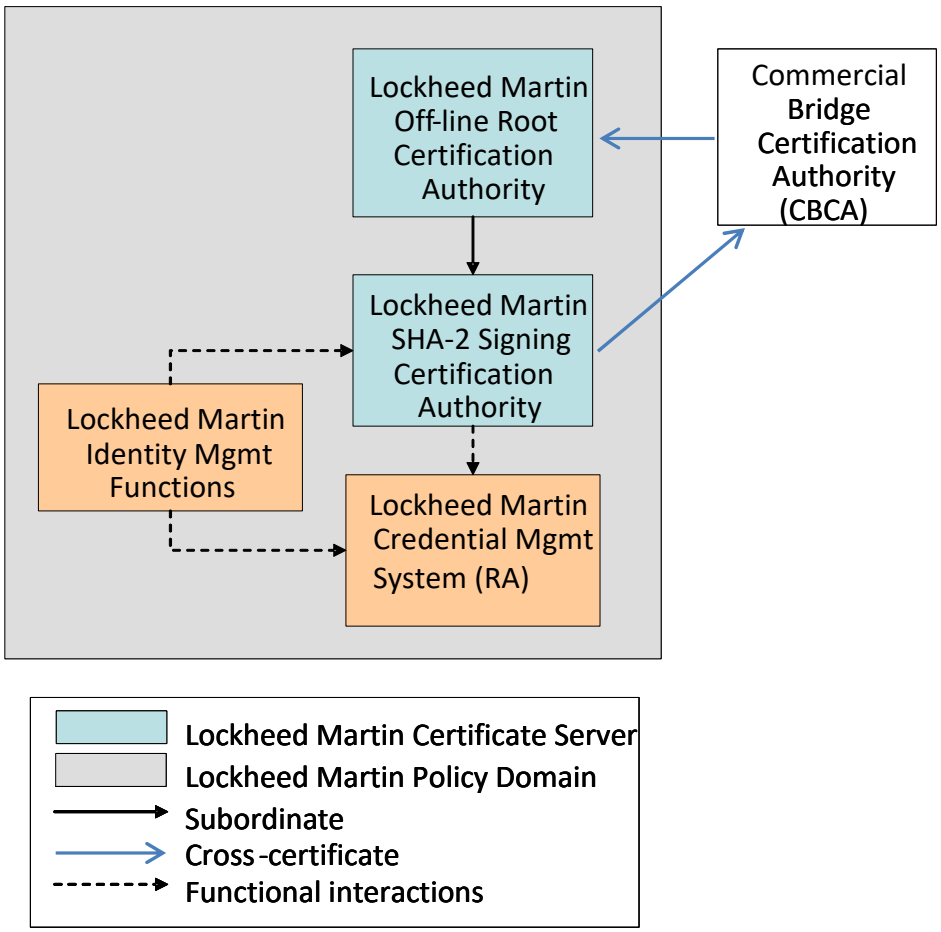

Figure 1 - LM's SHA-2 Public Key Infrastructure System Architecture

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

1.2 Document Identification

There are multiple levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance is associated with an OID, to be asserted in certificates issued by the Lockheed Martin Certification Authority, which comply with the policy stipulations herein.

The OIDs are registered under the Lockheed Martin Corporation private enterprise arc:

{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) Lockheed Martin(103)}

The OIDs associated with each level of assurance are listed below.

Assurance Level	**OID**
Medium Assurance Hardware Certificate	1.3.6.1.4.1.103.100.1.1.3.3
Medium Assurance Software Certificate	1.3.6.1.4.1.103.100.1.1.3.4

Assurance Level	OID
Medium Assurance Derived Certificate	1.3.6.1.4.1.103.100.1.1.3.5
Medium Assurance Hardware Device Certificate	1.3.6.1.4.1.103.100.1.1.3.6
Medium Assurance Software Device Certificate	1.3.6.1.4.1.103.100.1.1.3.7

This LM CP only governs Medium Assurance Software, Medium Assurance Hardware, Medium Assurance Derived, Medium Assurance Software Device and Medium Assurance Hardware Device issuance policies. The CAs may issue certificates that do not assert these OID values. However, such certificates will not be governed by this particular CP.

The requirements associated with the "Medium Assurance Hardware Device Certificate" and "Medium Assurance Software Device Certificate" policies are identical to those defined for other medium assurance policies with the exception of identity proofing, backup and activation data. The use of these policies is restricted to devices and systems (e.g., software applications and hardware devices). Certificates issued to end-entity devices shall assert one or both of the following policies: "Medium Assurance Hardware Device Certificate", "Medium Assurance Software Device Certificate". Other devices (such as content signers, OCSP responders, etc.) may assert appropriate policy OIDs.

1.3 PKI Participants

This section contains a description of the roles relevant to the administration and operation of the Lockheed Martin US Signing CA.

1.3.1 PKI Authorities

1.3.1.1 Lockheed Martin Policy Management Authority (LM PMA)

The LM PMA is responsible for:

- Overseeing the creation of and updates to the Lockheed Martin Certificate Policy (CP) and plans for implementing any accepted changes;
- Providing timely and responsive coordination to approved Business Unit PKI CAs
- Reviewing the Certification Practice Statements (CertPS) of the CA that provides services meeting the stipulations of this CP,
- Providing notification of changes that have the potential to affect the operations and/or security environments of cross certified entities to those cross-certified entities at least two (2) weeks prior to implementation, and,
- Reviewing the results of CA compliance audits to determine if the CA is adequately meeting the stipulations of this CP and associated approved CertPS documents, and making recommendations to the CA regarding corrective

actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CP.

The LM PMA will consist of representatives from Corporate Information Security (CIS) and Technical Operations (Tech Ops) organizations as well as representatives from each of the Business Areas, Legal, and Enterprise Operations.

In the event the LM Signing CA cross-certifies with another organization's CA, LM shall first enter into an agreement with that organization setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP. The stylized term AGREEMENT as used in this CP shall always refer to the agreement cited in this paragraph.

1.3.1.2 Lockheed Martin Operational Authority (OA)

The Lockheed Martin Operational Authority is the organization that operates and maintains the Lockheed Martin Certification Authority, including issuing certificates, posting those certificates and Certificate Revocation Lists (CRLs) into the Lockheed Martin Repository, and ensuring the continued availability of the repository to all users. The Operational Authority acts upon approval of the LM PMA.

1.3.1.3 Lockheed Martin Operational Authority Administrator (OAA)

The Operational Authority Administrator is the individual(s) within the Operational Authority who has principal responsibility for overseeing the proper operation of the Lockheed Martin CAs, including the Repository, and who appoints individuals to the positions of Operational Authority Officers. The administrator approves the issuance of certificates to the other trusted roles operating the Lockheed Martin CAs.

1.3.1.4 Lockheed Martin Operational Authority Officers (OAO)

These officers are the individuals within the Operational Authority, selected by the Operational Authority Administrator (OAA), who operate the Lockheed Martin CA and the Repository including executing the LM PMA direction to take actions to affect interoperability. The roles include Administrator, Officer, Audit Administrator, and Operator, all described in Section 5.2.1 of this CP.

Upon LM PMA approval of the issuance of CA certificates, the OAO will act to issue those certificates.

1.3.1.5 Lockheed Martin Principal Certification Authority (PCA)

The Lockheed Martin Principal CA is the LM Root or Signing CA operated by the OA that is designated to cross-certify directly with the CertiPath and/or TSCP (or other LM PMA-Approved Bridge Authority's) Commercial Bridge Certification Authority (CBCA) through the exchange of cross-certificates.

1.3.1.6 Root CA

The LM Offline Root CA is the trust anchor for LM relying parties.

The LM Offline Root CA cross-certifies with the Commercial Bridge Certification Authority.

1.3.1.7 Signing CA

The LM Signing CA is a CA whose primary function is to issue certificates to the end entities. It also issues cross-certificates to CBCAs that LM desires to establish qualified subordinated trust with.

The Signing CA does not issue any other type of CA certificate.

1.3.1.8 Cross-certified CA

A cross-certified CA is an organization that is operating a CA that has cross-certified with LM through the LM Signing CA.

1.3.1.9 Lockheed Martin Certificate Status Authority (CSA)

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

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates
- Simple Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services[1]

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

1.3.1.10 Key Recovery System (KRS)

The Key Recovery System consists of the information system (or systems) and operations personnel used to provide key escrow and key recovery services.

The KRS consists of the Key Escrow Database (KED) and Key Recovery Workstation and may include one or more Data Decryption Servers (DDS). KRS personnel include the Key Recovery Agents (KRA) and, optionally, Key Recovery Officers (KRO).

The applicable requirements for physical, personnel, and procedural security controls, technical security controls and Compliance Audit apply as follows:

- CA requirements apply to the KED and to the (optional) DDS
- RA requirements apply to the KRA and KRA automated systems
- RA requirements apply to the KRO and KRO automated systems, when the KRO has privileged access to the KED.

[1] There are three types of SCVP Servers: path development, path validation and revocation checking. The path development servers are not considered within the scope of this policy since the corruption of these servers does not adversely impact security and hence they need not be subject a CP.

1.3.1.10.1 Key Escrow Database (KED)

The Key Escrow Database is the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more key recovery trusted role personnel (e.g., KRAs) or card-management-system-facilitated recovery on the behalf of a current Certificate Holder.

Practice Note:
In some cases, the Registration Authority System may incorporate key escrow services. If so, the Registration Authority System must include the provision for preserving the enforcement of two-person integrity of key recovery operations.

1.3.1.10.2 Key Recovery Workstation

Key Recovery Workstations are used by the key recovery trusted role personnel to securely communicate with the KED for the recovery of escrowed keys.

1.3.1.10.3 Data Decryption Server (DDS)

Also known as a Key Server, the Data Decryption Server is an automated system that obtains Certificate Holder private keys or session keys from the KED or from another Key Server for data monitoring or other purposes (e.g., email inspection). A DDS does not provide keys to Certificate Holders or other Third-Party Requestors. A DDS must adhere to physical, personnel, procedural and technical security requirements of the KED. Lockheed Martin may use a DDS, if organizational needs arise.

1.3.1.11 Administration Workstation

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

1.3.2 Registration Authority (RA)

A Registration Authority (RA) is comprised of the systems, procedures and personnel that collect and verify each Subscriber's proof of identity and the subject information that is to be entered into the associated public key certificate. The RA interacts with the CA to enter and approve the certificate holder certificate request information. The RA performs its function in accordance with a CertPS approved by the LM PMA.

An RA may assume the duties of a Key Recovery Agent or Key Recovery Officer for the recovery of escrowed private decryption keys on behalf of Subscribers and third-party requestors or these roles may be assigned to separate personnel:

1.3.2.1 Key Recovery Agent (KRA)

A Key Recovery Agent is an individual who, using a two-party control procedure with a second KRS trusted role individual, is authorized to interact with the KED in order to recover an escrowed key. Because KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled. KRAs are considered Trusted Role personnel.

Two KRS trusted role individuals are required for a successful key recovery.

In addition, KRAs shall authenticate the Key Recovery Requestor and validate the requestor's authorization to recover keys when KROs are not used.

1.3.2.2 Key Recovery Officer (KRO)

Lockheed Martin may choose to use the services of a Key Recovery Officer (KRO) to perform identity verification and authorization validation tasks in support of key recovery. KROs authenticate the identity of the Key Recovery Requestor.

KROs perform their duties from a workstation that securely communicates with the KRA. A KRO performs the following:

- Authentication of the requestor;
- Validation of the requestor's authorization;
- Secure transmission of key recovery requests to a KRA.

When KROs are not used, authentication of the requestor and validation of the requestor's authorization to recover keys are the responsibility of the KRA.

1.3.3 Certificate Holder

The Certificate Holder is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. Lockheed Martin Certificate Holders include only Lockheed Martin subjects and resources. CAs are sometimes technically considered 'certificate holders' in a PKI. However, the term "Certificate Holder" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.1 Key Recovery Requestor

A Key Recovery Requestor is the person who requests the recovery of a decryption private key. A Requestor is generally the Certificate Holder itself (for self-recovery) or a third-party (e.g., supervisor, corporate officer, or law enforcement officer) who is authorized to request recovery of a Certificate Holder's escrowed key. Any individual who can demonstrate verifiable authority and a need to obtain a recovered key can be considered a Key Recovery Requestor.

1.3.3.1.1 Internal Third-party Requestor

An Internal Third-party Requestor is any Requestor who is in the Certificate Holder's supervisory chain or otherwise authorized to obtain the Certificate Holder's key on behalf of Lockheed Martin. Lockheed Martin shall appoint authorized Internal Key Recovery Requestors and the PKI shall implement key recovery such that the existing LM Corporate Policy regarding access and release of sensitive information is met.

1.3.3.1.2 External Third-party Requestor

An External Third-party Requestor is someone outside of Lockheed Martin with authorization from Lockheed Martin's legal department to obtain the decryption private key of the Certificate Holder. An External Key Recovery Requestor must work with an Internal Key Recovery Requestor unless the law requires the KRA to release the Certificate Holder's private key without Lockheed Martin's approval. Nothing in this document is intended to change Lockheed Martin's current Corporate Policy for obtaining information about individuals in connection with such requests.

Practice Note: The authorization process is determined by Lockheed Martin and may include the requirement for authorized court orders or other demonstrable legal rights to the information, and requests from customer organizations.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Certificate Holder'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 certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

1.3.5.1 Related Authorities

The LM Offline Root CA and LM Signing CA operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The Lockheed Martin CertPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.5.2 Trusted Agent

A Trusted Agent is appointed by PKI Operational Authority authorized personnel and may collect and verify Certificate Holder identity and information on behalf of an RA. A Trusted Agent may be an entity certified by a State or Federal Entity as being authorized to confirm identities. Information shall be verified in accordance with Section 3.2 and communicated to the RA in a secure manner. A Trusted Agent shall not have privilege on the CA to enter or approve certificate holder information.

When Trusted Agents are used, the Lockheed Martin Certification Practices Statement (CertPS) must include any criteria associated with the appointment of the Trusted Agent, to include vetting and training or certification (e.g. notary public). Identity proofing artifacts produced by a Trusted Agent must be traceable to the individual that produced them.

1.3.5.3 PKI Sponsor

A PKI Sponsor fills the role of a Certificate holder for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the Trusted Agent to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.2, and is responsible for meeting the obligations of Certificate holders as defined throughout this document.

1.3.6 Applicability

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

To provide sufficient granularity, this CP specifies security requirements for the Medium level of assurance which has two variants: Medium Hardware and Medium Software. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations.

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

Assurance Level	Applicability
Medium-software*	This level is relevant to environments where risks and consequences of data compromise are considerable. 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. Certificate holder private keys are stored in software at this assurance level.
Medium-hardware*	This level is relevant to environments where risks and consequences of data compromise are considerable. 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. Certificate holder private keys are stored in hardware at this assurance level.

* Medium Assurance Software allows for the Certificate holder private keys to be stored in software. Medium Assurance Hardware requires the Certificate holder private keys to be stored in hardware.

1.3.6.1 Factors in Determining Usage

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

1.3.6.2 Obtaining Certificates

This CP requires publication and access to CA certificates and CRLs. This CP imposes no requirements in terms of publication and access to end entity (i.e., certificate holder) certificates. The relying party applications must make their own agreement for obtaining the certificate holder certificates. This could be done trivially for signature applications by including the signer certificate in the application protocol. Use of X.500 and Lightweight Directory Access Protocol (LDAP) repositories is one way to achieve this, but neither this nor any other mechanism is mandated by this CP.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

None beyond those specified in Section 1.3.6.

1.4.2 Prohibited Certificate Uses

All certificates are considered Lockheed Martin assets and shall be used in accordance with all applicable corporate policies.

1.5 Policy Administration

1.5.1 Organization administering the document

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

1.5.2 Contact Point

Lockheed Martin Corporation
Attn: Lockheed Martin PKI Policy Authority Chair
CIS/Corporate Information Security Team
100 Global Innovation Circle
Bldg E8 MailDrop: 116
Orlando FL 32825-5003

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The LM PMA shall approve the Lockheed Martin CertPS. The CertPS must conform to this Certificate Policy.

The determination of suitability shall be based on an independent compliance assessor's results and recommendations. The compliance assessor shall be independent from Lockheed Martin's Enterprise PKI organization. The compliance assessor must not be the author of the subject CertPS. (See Section 8 for complete assessor requirements).

1.5.4 Certification Practice Statement (CertPS) Approval Procedures

The term CPS is defined in the Internet 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 lifecycle management. It shall be more detailed than the corresponding certificate policy described above. The Lockheed Martin Certification Practice Statement (CertPS), which is contained in a separate document published by the Operational Authority and approved by the LM PMA, specifies how this CP and any AGREEMENTS that the LM PMA has approved will be implemented to ensure compliance with their provisions.

1.5.5 Waivers

There shall be no waivers to this CP.

2 PUBLICATION & PKI REPOSITORY RESPONSIBILITIES

2.1 PKI Repositories

Lockheed Martin shall operate repositories to support Lockheed Martin PKI operations. The repositories shall be accessible by both internal and external relying parties. The Lockheed Martin repositories shall contain the information necessary to support successful PKI interoperation such as CA certificates, CRL files, and information on organizational policy (such as this Certificate Policy document itself).

The Lockheed Martin Operational Authority may use a variety of mechanisms for posting information into their respective 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, and
- Access control mechanisms, when needed to protect repository information, as described in later sections.

The PKI Repositories containing certificates and certificate status information shall be deployed so as to provide 24 hours per day/365 days per year availability. Lockheed Martin shall implement features to provide high levels of PKI Repository reliability (99% availability or better).

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

The Operational Authority shall publish information concerning the Lockheed Martin CAs necessary to support their use and operation.

All CAs, at a minimum, shall post CA certificates and CRLs to the PKI repository.

All CA certificates shall be posted in publicly accessible HTTP URIs.

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

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

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

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

> Practice Note: Internet disruptions are one example of an abnormal operating condition which may impact the response time experienced by the relying party.

2.2.2 Certificate Policy Publication

The Lockheed Martin Certificate Policy document shall be posted as a file available via a publicly accessible HTTP URI.

2.3 Time or Frequency of Publication

Certificate Policy updates (revisions) must be made publicly available within thirty (30) days of approval.

Certificates and certificate status information shall be published as specified in this CP in Section 4.

2.4 Access Controls on Repositories

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

Public keys and certificate status information in the external, HTTP-based Lockheed Martin PKI Repository shall be publicly available through the Internet.

3 IDENTIFICATION & AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

CAs shall generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields; the X.500 DN may contain domain component elements. Subject Alternative Name may be used, if marked non-critical.

3.1.1.1 Subject Names

For certificates issued to human Certificate Holders, the subject DN shall contain the affiliated organization name in an appropriate relative distinguished name attribute (e.g., organization (o), organizational unit (ou), or domain component (dc) attribute).

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

3.1.1.2 Subject Alternative Names

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

For Device Certificate Holder certificates that assert serverAuth in the Extended Key Usage:

- Wildcard domain names are permitted in the dNSName values only if all sub-domains covered by the wildcard fall within the same application, cloud service, or system boundary within the scope of the sponsoring organization.
- Wildcards shall not be used in subdomains that host more than one distinct application platform.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

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

When DNs are used, it is preferable that the common name represents the certificate holder 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/or serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

3.1.3 Anonymity or Pseudonymity of Certificate holders

CA certificates shall not contain anonymous or pseudonymous identities.

DNs in certificates issued to Certificate Holders may contain a pseudonym to meet local privacy regulations provided that name space uniqueness requirements are met and such name is traceable to the specific Certificate Holder.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile. The LM PMA shall be the authority responsible for CA name space control.

3.1.5 Uniqueness of Names

Name uniqueness across the Lockheed Martin domains, including cross-certified domains shall be enforced. Each name shall be unique and for a single unique entity. The CAs and RAs shall enforce name uniqueness within the X.500 name space, for which they have been authorized.

The LM PMA shall be responsible for ensuring name uniqueness in certificates issued by the Lockheed Martin CAs.

Lockheed Martin shall include the following information in its CertPS:

- What name forms shall be used, and
- How they will allocate names within the Certificate holder community to guarantee name uniqueness among current and past Certificate holders (e.g., if “Joe Smith” leaves a CA community of Certificate holders, and a new, different “Joe Smith” enters the community of Certificate holders, how will these two people be provided unique names?).

3.1.6 Recognition, Authentication & Role of Trademarks

Lockheed Martin supports the inclusion of trademarks in names provided that the subject has the right to use the trademark being included in the name.

3.1.7 Name Claim Dispute Resolution Procedure

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

3.2.2 Authentication of Organization Identity

Requests for cross certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing cross certificates, the LM PMA shall verify the information provided, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.3 Authentication of Individual Identity

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

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

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

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

3.2.3.1 Authentication of Human Certificate Holder Identity

Identity shall be established by in-person or supervised remote[2] identity proofing before the RA, Trusted Agent, or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy.

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

The CA or RA shall ensure that the applicant's identity information is verified and checked in accordance with the applicable level of assurance as detailed in the CertPS. The CA or an RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance

---

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

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

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

- The identity of the person performing the identity verification and either:
  - A signed declaration by that person that the identity of the applicant was verified 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, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued; or
  - An auditable record linking the authentication of the person performing the identification to the verification of each Applicant.
- Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant or, in the case of electronic authentication, the serial number, subject key identifier, public key or other unique identifier from the certificate used to authenticate the request;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) 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: In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity then the certificate must be revoked.

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

3.2.3.2 Authentication of Device Identities

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device shall have a human PKI Sponsor. The PKI Sponsor should have been issued a credential that is equal to or higher in assurance level than the credential being sponsored. The PKI sponsor shall be responsible for the security of the private key and for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys

- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information provided by the human sponsor 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 sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

In the event a human sponsor is changed, the new sponsor shall review the status of each sponsored device to ensure it is still authorized to receive certificates. The CertPS shall describe procedures to ensure that certificate accountability is maintained.

3.2.3.3 Human Certificate holder Re-Authentication following loss, damage, or key compromise

If any computing device, token, or smart card containing a human certificate holder's private keys is lost, damaged, or stolen, the certificate holder may be issued new certificates. The certificate holder must undergo the initial identity proofing process described in Section 3.2.3.1.

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. 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) shall also be revoked.

3.2.3.4 Human Certificate holder Initial Identity Proofing Via Antecedent Relationship

Lockheed Martin shall not perform initial identity proofing via antecedent and instead shall only perform initial identity proofing as described in section 3.2.3.1 of this CP.

3.2.3.5 Authentication of Human Certificate Holder for Role Certificates

Certificate Holders may be issued role certificates. A role certificate shall identify a specific role title on behalf of which the Certificate Holder is authorized to act rather than the Certificate Holder'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 Certificate Holder certificate. Multiple Certificate Holders can be assigned to a role at the same time; however, the signature key pair 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.

Certificate Holders issued role certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., Certificate Holder identity proofing, validation of organization affiliation, key generation, private key protection, and Certificate Holder 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 a role signature certificate shall require the approval of the role sponsor. Rekey and renewal of a 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 the RA shall record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role certificate. The role sponsor shall hold an individual certificate issued by the same CA at the same or higher assurance level as the role certificate. The CA or the RA shall validate from the role sponsor that the individual Certificate Holder 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. Recovery of the private decryption key
3. Revocation of individual role certificates;
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.

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

3.2.4 Non-verified Certificate holder Information

Certificate Holder information that is not verified shall not be included in Certificates.

3.2.5 Validation of Authority

The Issuer CA shall validate the subject CA certificate requestor's authorization to act in the name of the Subject CA. In addition, the LM CAs shall obtain the LM PMA approval prior to issuing CA certificates. Certificates 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

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

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

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

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

The following table shows how often the end entity that receives the certificate must be re-proofed:

Assurance Level	Length of time
Medium Software/Hardware	Every 12 years
Medium Device Software/Hardware	Every 12 years

For cross-certified CAs, as required in Section 3.2, identity shall be re-established through the initial registration process at least once every three years, see Section 3.2.2.

When a current public key certificate is used for identification and authentication purposes, the expiration date of the new certificate shall not cause the certificate subject to exceed the initial identity-proofing time frames specified in the table above; and the assurance level of the new certificate shall not exceed the assurance level of the certificate being used for identification and authentication purposes.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked, other than during a renewal or update action, the subject (i.e., a cross-certified CA or a Certificate Holder) is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Communication among the CA, RA, Trusted Agent, other parties confirming identities, and certificate holders 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. For example, packages secured and transported in a tamper-evident manner by a certified mail carrier meet the integrity and confidentiality requirements for the High assurance level. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, a web site secured using an TLS certificate issued under medium-software policy and set up with appropriate algorithms and key sizes satisfies integrity and confidentiality requirements for medium-software certificate management.

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

4.1 Certificate Application

This paragraph applies to entities seeking cross-certificates from the Lockheed Martin US Signing CA. The LM PMA shall establish procedures for entities to use in applying for a certificate from a Lockheed Martin US Signing CA and then publish those procedures. The application shall, at a minimum, be accompanied by a CP written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647]. Additional requirements for the enrollment process for cross-certified CAs shall be discussed in an AGREEMENT signed by the LM PMA. Lockheed Martin, based on LM PMA Chair recommendation, shall act on the application, and upon making a determination to issue a certificate and entering into the AGREEMENT with the applicant organization, shall instruct the Operational Authority to issue the certificate to the applicant CA. The applicant CA, known as the Principal Certification Authority (PCA) or the 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 certificate holder certificates, a Trusted Agent must perform the following steps when the certificate holder applies for a certificate:

- Establish and record identity of certificate holder (per Section 3.2)
- Establish that the public key forms a functioning key pair with the private key held by the certificate holder (per Section 3.2.1)

For certificate holder certificates, the prospective certificate holder must perform the following step when the certificate holder applies for a certificate:

- Obtain a public/private key pair for each certificate required

These steps (from both lists above) may be performed in any order that is convenient for the CA and Certificate holders and that do not defeat security; but all must be completed prior to certificate issuance. All communications among CAs supporting the certificate application and issuance process shall be authenticated and protected from modification

using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued (i.e., communications supporting the issuance of Medium Assurance certificates shall be protected using Medium Assurance certificates, or some other mechanism of equivalent strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

Requests for CA certificates by other internal Lockheed Martin CAs (i.e. a CA not managed by the Enterprise PKI OA) shall be submitted to the LM PMA using the contact provided in Section 1.5 and shall be accompanied by a CertPS written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647].

The LM PMA will evaluate the submitted CertPS for acceptability. The LM PMA may require an initial compliance audit, performed by parties of the PMA's choosing, to ensure that the CA is prepared to implement all aspects of the submitted CertPS, prior to the LM PMA authorizing the CA to issue and manage certificates asserting the Lockheed Martin CP.

4.1.1 Submission of Certificate Application

For CA certificate applications to a Lockheed Martin CA, an authorized representative of the Subject CA shall submit the application to the LM PMA.

For certificate holder certificates, the application shall be submitted by an authorized prospective certificate holder in the case of human certificate holders, or an authorized PKI sponsor in the case of devices.

4.1.2 Enrollment Process and Responsibilities

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

CAs external to the Lockheed Martin policy domain applying for cross-certification with the Lockheed Martin PKI shall submit a request for cross-certification to the LM PMA accompanied by their CP. The LM PMA shall require a CP/CertPS compliance audit, from a third-party auditor, as described in section 8. The LM PMA shall perform a certificate policy mapping to validate policy assurance levels are equivalent. Upon issuance, each cross-certificate issued by the Lockheed Martin PKI 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.

Lockheed Martin CAs shall submit a request to the LM PMA, accompanied by their CertPS. The LM PMA shall evaluate the submitted CertPS for acceptability. The LM PMA may require an initial compliance audit, performed by parties of the LM PMA's choosing, to ensure that the CA is in compliance with this CP, prior to the PMA authorizing the Lockheed Martin Root CA to issue a certificate to the applying CA and authorizing the CA to issue and manage certificates asserting a policy OID from this CP.

The Lockheed Martin Root CA shall issue certificates to subordinate CAs only upon receipt of written authorization from the LM PMA.

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

For applications by end-entities, the Trusted Agent must verify all certificate holder information, in accordance with section 3.2.3. In addition, the Trusted Agent shall sign the RA/Certificate holder agreement.

Certificate holders are expected to present proof of identity commensurate with the Assurance Level of the certificate being requested to Trusted Agents, to electronically agree to the certificate holder agreement, and to sign it with a handwritten or electronic signature.

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

4.2 Certificate Application Processing

It is the responsibility of the Trusted Agent and/or RA to verify that the information in certificate applications is accurate. Information in certificate applications must be verified as accurate before certificates are issued. The applicable CertPS shall specify procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

For the cross-certificate issued by the Lockheed Martin Signing CA, which is subordinate to the LM Root CA that will be cross-certified with the CertiPath and/or TSCP (or other LM PMA-Approved Bridge Authority's) Commercial Bridge Certification Authority (CBCA), the identification and authentication of the applicant representing the CBCA shall be performed by the LM PMA.

For end entity certificates issued by the Lockheed Martin Signing CA, the identification and authentication of the Certificate holder must meet the requirements specified for Certificate holder authentication as specified in Sections 3.2 and 3.3 of this CP.

For the Lockheed Martin CAs, the identification and authentication of the applicant representing the Lockheed Martin CA shall be performed by the LM PMA.

4.2.2 Approval or Rejection of Certificate Applications

For CA certificates, the LM PMA may approve or reject a certificate application.

For certificate holder certificates, the Trusted Agent, Human sponsor, RA, or CA may approve or reject a certificate application.

4.2.3 Time to Process Certificate Applications

The entire certificate issuance process (from the time the request/application is posted on the CA or RA system to certificate issuance) shall not exceed 90 days.

4.3 Certificate 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 corresponding CertPS.

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

While the Certificate holder may do most of the data entry for a certificate, it is still the responsibility of the Trusted Agent 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 Certificate holder's sponsoring organization. If databases are used to confirm Certificate holder information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought. Specifically, the databases shall be protected using physical security, personnel controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

4.3.1 CA Actions during Certificate Issuance

The CA shall:

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

4.3.2 Notification to Certificate holder of Certificate Issuance

The CA shall notify a subject (CA or Certificate holder) of certificate issuance. When a key management (encryption) certificate is issued, the Subscriber shall be notified that the associated private decryption keys will be escrowed.

4.4 Certificate Acceptance

The AGREEMENT shall set forth responsibilities of all parties before the LM PMA authorizes issuance of a cross-certificate by a Lockheed Martin CA. Once a CA certificate has been

issued, its acceptance by the subject shall trigger the Subject CA's obligations under the applicable AGREEMENT (if any) and this CP.

Certificate Holders shall accept the responsibilities defined in Section 9.6.2 by signing the Certificate Holder agreement during certificate issuance.

4.4.1 Conduct Constituting Certificate Acceptance

For CAs cross-certified with Lockheed Martin, conduct constituting certificate acceptance shall be spelled out in the AGREEMENT between Lockheed Martin and the representatives of the cross-certified CA.

For Lockheed Martin 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 end-entities, acceptance of the certificate shall be accomplished by one of the following:

1. Downloading of the certificate
2. Receiving the certificate on a hardware token, such as a smart card

For electronic authentication for certificates, such as server certificates, the Certificate holder request to obtain new certificates and subsequent failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

All CA certificates shall be published in a PKI Repository accessible over the Internet.

4.4.3 Notification of Certificate Issuance by the CA to Other entities

The LM PMA and all cross-certified entities shall be notified upon issuance of new CA certificates by the Lockheed Martin PKI. In addition, the new CA certificate(s) shall be provided to the cross-certified entities.

In the event a CA renews, rekeys or modifies a certificate without interaction with the RA system involved in the existing certificate’s issuance, the CA must notify the RA of the action taken.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate holder Private Key and Certificate Usage

Certificate holders and CAs shall protect their private keys from access by any other party.

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

4.6 Certificate Renewal

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

After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if it has not reached the end of its validity period and has not been revoked, the associated private key has not been compromised, and the Certificate holder name and attributes are unchanged. The validity period of the new certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3.1 shall also be met.

CA certificates and Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 5.6.

4.6.2 Who may Request Renewal

The Lockheed Martin Operational Authority Manager may request renewal of cross-certificates.

A Subject may request the renewal of its certificate.

A PKI Sponsor may request renewal of a device certificate.

A RA may request renewal of a Certificate Holder certificate.

A CA may request renewal of its certificate holder certificates, e.g., when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

Requests for certificate renewal of the Lockheed Martin Signing CA or cross-certified CAs, for reasons other than re-key of the Lockheed Martin Root CA, shall be approved by the LM PMA.

For cross-certificates issued by a Lockheed Martin Signing CA, certificate renewal also requires that a valid AGREEMENT exists between the LM PMA and the cross-certified CA, and the term of the AGREEMENT is beyond the expiry period for the new certificate.

A certificate renewal shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

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

4.6.4 Notification of New Certificate Issuance to Certificate holder

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. After certificate rekey, the old certificate may or may not be revoked, but must not be used for requesting further re-keys, renewals, or modifications.

4.7.1 Circumstance for Certificate Re-key

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

4.7.2 Who may Request Certification of a New Public Key

A Subject may request the re-key of their own certificate.

A PKI Sponsor may request re-key of a device certificate.

4.7.3 Processing Certificate Re-keying Requests

For cross-certificates issued by the Lockheed Martin US Signing Certificate Authority, certificate re-key requires that a valid AGREEMENT exists between the Lockheed Martin US Signing Certificate Authority and the Subject CA, and the term of the AGREEMENT is beyond the expiry period for the new certificate.

For CA certificates issued by the Lockheed Martin Root CA, certificate re-key requests must be submitted to the LM PMA by an authorized representative of the CA.

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

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

4.7.4 Notification of New Certificate Issuance to Certificate holder

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

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

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) for a modified certificate containing the new name to be issued.

Certificates issued by the Lockheed Martin PKI shall not be modified.

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 Certificate holder

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised*.*

Lockheed Martin shall notify all cross-certified entities at least two weeks prior to the revocation of a CA certificate, whenever possible.

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

4.9.1 Circumstance 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 in the certificate becomes invalid;
- Privilege attributes asserted in the Subject's certificate are reduced;
- The Subject can be shown to have violated the stipulations of its agreement;
- The private key is suspected of compromise; or
- The Subject or other authorized party (as defined in the applicable CP or CPS) asks for the 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.

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

4.9.2 Who Can Request Revocation of a Certificate

A certificate subject, human supervisor of a human subject, Human Resources (HR) representative for the human subject, PKI Sponsor for a device, Signing CA, RA, Legal, or Trusted Agent may request revocation of a certificate.

For CA certificates, the LM PMA and/or authorized individuals representing the CA operations may request revocation of certificates.

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 Operational Authority for a LM CA shall revoke a Subject CA certificate only in the case of an emergency. Generally, the certificate will be revoked based on the subject request, authorized representative of subject request, or LM PMA request.

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

- Request from the Subject CA for reason of key compromise;
- Determination by the Operational Authority that a Subject CA key is compromised; or
- Determination by the Operational Authority that a Subject CA is in violation of the CP or CertPS.

At the medium-hardware assurance level, a Certificate holder ceasing its relationship with Lockheed Martin shall, prior to departure, surrender to Lockheed Martin (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of Lockheed Martin. 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 Certificate holder leaves Lockheed Martin and the hardware tokens cannot be obtained from the Certificate holder, then all Certificate holder 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 Lockheed Martin Offline Root CA shall process all revocation requests within six hours of receipt of request.

For LM Signing CAs operating under this policy, revocation request processing time is specified below:

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

*Revocation requests received within two hours of CRL issuance must be processed before the following CRL is published.

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 should either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA shall ensure that superseded certificate status information is removed from the 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. The LM OA shall coordinate with the 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 and medium-hardware assurance certificates.

	CRL Issuance Frequency
Routine	CAs that are offline and do not issue end-entity certificates except for internal operations must issue CRLs at least monthly; At Least Once every 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 LM Operational Authority and cross-certified Partner Operational Authorities upon Emergency CRL issuance. The LM Operational Authority shall in turn notify the LM PMA of revocation.

For off line Root CAs, the nextUpdate shall be less than or equal to thisUpdate plus 45 days.

For all other CAs, the nextUpdate shall be less than or equal to thisUpdate plus 168 hours.

4.9.8 Maximum Latency for CRLs

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

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

4.9.9 Online Revocation Checking Availability

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

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

4.9.10 Online Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Related To Key Compromise

None beyond those stipulated in Section 4.9.7.

4.9.13 Circumstances for Suspension

Suspension shall not be used.

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

Lockheed Martin CAs do not support any other certificate status services.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

For certificates that have expired prior to or upon end of subscription, revocation is not required. Unexpired CA certificates shall always be revoked at the end of the subscription.

4.12 Key Escrow and Recovery

When encryption certificates are issued by an LM CA covered by this policy, the private key shall be escrowed. LM shall offer key escrow and recovery capability.

Escrowed keys should be maintained within the KED for a period of time that satisfies organizational and regulatory requirements, in no case shall the period of retention be less than one year after the expiration of the associated public key certificate.

Certificate Holders shall be notified that their private decryption keys are escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall a CA or end entity user private signature key be escrowed.

Key Recovery practices for private decryption keys must satisfy the privacy and security requirements for the CAs that issue and manage the corresponding key management public key certificates.

4.12.1.1 Key Escrow Process and Responsibilities

Escrowed keys shall be transmitted to and stored in a KED for which the protection mechanisms provide a level of security equal to or greater than that at which the private decryption keys are generated, delivered to and protected by the Certificate Holder.

KRAs and KROs shall not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless authorized by this CP; required by law, government rule, or regulation; by the Certificate Holder's Organization/Enterprise policy; or by order of a court of competent jurisdiction.

4.12.1.2 Key Recovery Process and Responsibilities

Certificate Holders may request recovery of their own escrowed keys. Key recovery may also be requested by the personnel permitted by the Certificate Holder's organization policy to recover subscriber keys and by authorized law enforcement personnel with a court order from a competent court.

Requestor identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered.

Lockheed Martin may implement automated self-recovery for Certificate Holders seeking the recovery of their own escrowed keys. In all other cases, key recovery requires a KRA to validate the identity and authenticate the authority of the requestor to request the key recovery.

When Requestor authentication and authorization verification is delegated to a KRO, the KRO must hold a Medium Assurance Hardware certificate issued by Lockheed Martin. The KRO shall provide proof of identity and authorization to the KRA as part of the key recovery request. KRAs shall authenticate the identity of the KRO before accepting and processing a request for key recovery. If the requestor digital signature is available, KRAs shall also authenticate the identity of the requestor, i.e., when the requestor makes an electronic request that is digitally signed, the KRO shall forward the requestor digital signature in a form verifiable by the KRA. In addition, KRAs may request additional information or verification from the KROs if deemed necessary.

When a KRA or KRO initiates a key recovery request for a Requestor, the requestor is generally a third-party, but this CP does not preclude the Certificate Holder from seeking the assistance of a KRA or KRO to recover the Certificate Holder's private key.

With the exception of self-recovery, the following requirements apply to key recovery:

- A Certificate Holder's escrowed keys shall be recovered only upon receipt of a request from an authorized requestor.
- The identity of any requestor seeking a key recovery shall be validated. The process for validating the identity shall be the same as the one used for identity proofing as defined in Section 3.2.3 or 3.2.3.1.
- A digital signature may be accepted as proof of identity provided the associated certificate is issued by Lockheed Martin, the certificate has not expired, is not

revoked, and is for the same or greater assurance level than the certificate associated with the key in the recovery request. In addition, the requestor's authorization to recover the specific keys in this request shall be verified.
- When a KRO performs the requestor authentication and authorization validation, the KRO sends the key recovery request to the KRA.
- The KRAs shall verify the request and perform the key recovery in a manner that ensures that at no point during the recovery process shall a single individual control both the recovered key and the decryption material.

Notwithstanding the above, if recovery is performed by a KRA in support of a forensic investigation, that KRA may control both the recovered key and the decryption material.

- The recovered key and information required to decrypt the key are provided to the Requestor by separate channels. If the Requestor retrieves the recovered key in person, one KRA shall deliver the encrypted recovered key, while the other KRA shall deliver the information required to decrypt the key. For electronic retrieval, the recovered key is sent via protected channel and in encrypted form to the Requestor. Information required to decrypt the recovered key is provided to the Requestor by a separate channel. The Requestor shall acknowledge receipt of the recovered key.
- KROs and KRAs shall protect all information regarding all occurrences of key recovery. They shall not communicate any information concerning a key recovery to the Certificate Holder except when the Certificate Holder is the requestor.
- Records of all recovery requests and their disposition shall be retained, including acknowledgement of receipt by the requestor. The audit records shall not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

During delivery, recovered keys shall be protected against disclosure to any party except the requestor in a manner commensurate with the level of assurance of the associated certificate.

4.12.1.2.1 Third-party Requestors Identity Proofing and Authentication

The LM PMA shall determine how third-party requests for recovery of decryption keys are managed. For example, the external third-party requestor may be required to establish its identity to an authorized organizational representative who will then act as an internal third-party requestor for the recovery of the requested decryption key.

The internal third-party requestor shall establish its identity to the KRA or KRO using one of the following methods:

- In-person using the process described in Section 3.2.3.1; or
- On the basis of an electronically authenticated request using a valid signature or authentication private key and associated certificate issued by Lockheed Martin at an assurance level equal to or higher than the certificate associated with the escrowed key to be recovered.

The antecedent process shall not be used. The authority of the requestor to recover the requested key shall be verified prior to initiating the key recovery request, in consultation with Lockheed Martin management and/or legal counsel, as appropriate.

> Practice Note: Lockheed Martin will determine internal notification requirements for External Third-Party key recovery requests and provide a provision for situations where the law requires the KRA to release a Subscriber's private decryption key without organizational notification.

4.12.1.2.2 Certificate Holder Identity Proofing and Authentication

With the exception of automated self-recovery, Certificate Holders shall establish their identities to the KRA or the KRO prior to initiation of the key recovery request using one of the following processes:

- In-person using the process described in Section 3.2.3.1; or
- On the basis of an electronically authenticated request using a valid signature or authentication private key and associated certificate issued by Lockheed Martin at an assurance level equal to or higher than the certificate associated with the escrowed key to be recovered.

For automated self-recovery, the Certificate Holder must be authenticated to the KED using a valid authentication private key and associated certificate issued by Lockheed Martin. The certificate policy assurance level of the authentication certificate shall be equal to or greater than that of the certificate associated with the private key being recovered.

4.12.1.2.3 KRA and KRO Authentication

The KRA shall authenticate to the KED directly using a public key certificate issued by Lockheed Martin. The assurance level of the certificate shall be the same as or greater than that of the certificate whose associated private key is being recovered.

The KRO shall authenticate to the KRA using a public key certificate issued by Lockheed Martin. The assurance level of the certificate shall be the same as or greater than that of the certificate whose associated private key is being recovered. The KRA shall verify that the KRO is authorized to request recovery of keys associated with the identified Subscriber.

4.12.1.2.4 DDS Authentication

The Data Decryption Server (DDS) shall authenticate to the KED directly using a public key certificate issued by Lockheed Martin. The assurance level of the certificate shall be the same as or greater than that of the highest-level encryption certificates associated with the private decryption keys escrowed in the KED.

The KED shall verify that the DDS is authorized to obtain the keys for the claimed subscriber community.

4.12.1.2.5 Operational Requirements

Recovery of Escrowed keys on behalf of a Certificate Holder is permitted in the case where Escrowed keys are recovered in order to populate a token's key history during new

certificate or new hardware token issuance. Additionally, former Certificate Holders who no longer possess an active authentication certificate may request recovery of their own escrowed keys from the KRA or KRO. Certificate Holder identity verification shall be performed in accordance with Section 4.12.1.2.2.

Internal third-party requestors shall submit key recovery requests to the KRA or KRO. Identity verification of the third-party requestor shall be performed in accordance with Section 4.12.1.2.1. The third-party requestor shall provide proof of authority to recover the subject key. Such proof of authority shall be verified by the KRA or KRO.

A DDS shall use electronic means to request Certificate Holders' escrowed keys. Requests shall be authenticated using a process at least as strong as the key being recovered. See Section 4.12.1.2.4.

In all cases, recovered keys must be protected against disclosure to any party except the requestor during transport and delivery.

4.12.1.2.5.1 KRS Operational Security

Communications between and among the KED, KRAs, KROs, DDS, and Requestors shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism shall ensure that the recipient and the transmitting party are the only holders of this shared secret.

4.12.1.2.5.2 Key Recovery through KRA

The KRA shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the actions of at least two KRAs. All copies of escrowed keys shall be protected continuously using two-person control procedures during recovery and delivery to the authenticated and authorized requestor. Split key or password procedures are considered adequate two person controls.

The delivery mechanism for copies of recovered keys shall provide cryptographic protection against disclosure with an assurance equal to or greater than the assurance level of the certificates associated with the escrowed keys.

Notwithstanding the above, if recovery is performed by a KRA in support of a forensic investigation, that KRA may control both the recovered key and the decryption material.

4.12.1.2.5.3 Automated Self-Recovery

Currently, Lockheed Martin does not offer automated self-recovery to Certificate Holders.

If, in the future, Lockheed Martin does offer automated self-recovery to Certificate Holders, then current Certificate Holder's escrowed keys may be provided directly to that Certificate

Holder using automated self-recovery without imposition of two-person control requirements.

The delivery mechanism for copies of self-recovered keys shall provide cryptographic protection against disclosure with an assurance level equal to or greater than the certificates associated with the escrowed keys.

The KED shall provide self-recovery of escrowed keys to current Certificate Holders only after:

- Verifying that the authenticated identity of the requestor is the same as the Certificate Holder associated with the escrowed keys being requested.
- Attempting to notify the Certificate Holder of all attempts (successful or unsuccessful) to use the automated self-recovery process to recover the Certificate Holder's escrowed keys. If the KED does not have information (e.g., an email address) necessary to attempt to notify the Certificate Holder of a key recovery request, then the KED shall not provide the Certificate Holder with the requested key material using the automated recovery process.
- Ensuring that the recovered keys are being sent only to the authenticated Certificate Holder associated with the escrowed keys; and
- Ensuring that the recovered keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

When self-recovery involves delivering the escrowed key directly to the Certificate Holder's hardware token, the KED shall use a secure means (e.g., Global Platform Secure Channel Protocol, Mini-driver API, etc.) to inject the private key onto the hardware token directly. Once injected, the recovered key shall not be exportable from the hardware token.

4.12.1.2.5.4 Recovery by DDS

An escrowed key may be provided directly to the DDS provided the DDS is operated under continuous two-person control. The KED shall perform the following prior to releasing the key:

- Authenticate the requestor as a legitimate DDS.
- Verify that the DDS is authorized to recover the escrowed key for Lockheed Martin.
- Ensure that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than those provided by the escrowed keys.

A combination of physical, procedural, and technical security controls shall be used to enforce continuous two-person control on the DDS. Where feasible, the DDS shall be designed to use technical means to enforce two-person controls rather than physical or procedural means.

Practice Note: The DDS is considered under continuous two-person control when any human action performed on the DDS requires two persons.

4.12.1.2.5.5 Key Recovery During Token Issuance

Escrowed keys may be recovered in order to populate a token's key history during new certificate or new hardware token issuance. In this case, the KED shall use a secure means (e.g., Global Platform Secure Channel Protocol, Mini-driver API, etc.) to inject the key history onto the hardware token directly. Once injected, the recovered keys shall not be exportable from the hardware token.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session key recovery is not supported.

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location & Construction

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

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

5.1.2 Physical Access

5.1.2.1 CA Physical Access

CA, KED, DDS and CSA equipment, including any Administration Workstations, shall always be protected from unauthorized access. The physical security requirements pertaining to CA, KED, DDS and CSA equipment, including any Administration Workstations, are:

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

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or any removable hardware associated with Administration Workstations.

A security check of the facility housing the CA, KED, DDS or CSA equipment or the Administration Workstation shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- For off-line CA, 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; and
- The area is secured against unauthorized access.

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

5.1.2.2 RA and KRA Equipment Physical Access

RA and Key Recovery Workstations shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA and KRA 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 and KRA Workstation environment.

5.1.3 Power and Air Conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention & Protection

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

5.1.6 Media Storage

CA and KRS media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste Disposal

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

5.1.8 Off-Site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule and described in the respective CertPS. Backups shall be performed and stored off-site not less than once every 7 days, unless the CA is off-line, in which case, it shall be backed up whenever it is activated or every 7 days, whichever is later. At least one full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate with 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 and associated KRS is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

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

1. *Administrator* – authorized to install, configure, and maintain the CA and KRS; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. *Officer* – authorized to request or approve certificate issuance, certificate revocation, and key recovery.
3. *Audit Administrator* – authorized to view and maintain audit logs.
4. *Operator* – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.1.1 Administrator

The administrator shall be responsible for:

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

Administrators shall not issue certificates to certificate holders.

5.2.1.2 Officer

The officer shall be responsible for issuing certificates, that is:

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

5.2.1.3 Audit Administrator

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA and KRS are operating in accordance with their CertPS.

5.2.1.4 Operator

The operator shall be responsible for the routine operation of the CA and KRS 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;
- Entering Certificate holder information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Certificate Holder 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 CertPS.

5.2.1.6 Key Recovery Agent

The KRA shall be responsible for:

- Verifying a requestor’s identity and authorization;

- Enabling (i.e., initiating or approving) the recovery of copies of escrowed keys;
- Distributing copies of recovered escrowed keys to requestors, with appropriate protection.

Note: Lockheed Martin may choose to utilize KROs to perform requestor identity and authorization verification on behalf of the KRA. In such cases, the KRAs shall be responsible for monitoring KRO activity.

The individuals assigned to the CA Officer or RA trusted role also may be assigned to the KRA trusted role.

5.2.1.7 CSA Roles

A CSA shall require at least the following roles.

The CSA Administrator shall be responsible for:

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

The CSA Audit Administrator shall be responsible for:

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

The CSA Operator shall be responsible for:

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

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

5.2.2 Number of Persons Required per Task

Two or more persons shall be required to perform the following tasks:

- CA, KED, DDS and CSA Signing key generation;
- CA, KED, DDS and CSA Signing key activation;
- CA, KED, DDS and CSA Signing private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall 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 Role.

In addition to the above, with the exception of Certificate Holder self-recovery (where implemented), two or more KRAs are required to recover an escrowed key.

It is recommended that multiple persons are assigned to all roles in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

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

An individual in a trusted role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI. Two factor (or better) access control, where at least one factor is a hardware token shall be used for logon to the Administration Workstation. In addition, the hardware token used must be acceptable for the highest certificate policy OID supported by the associated CA. Also See Section 6.7 for authentication to the PKI enclave.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, shall be enforced either by the CA and RA equipment/software, or procedurally, or by both means.

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

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

In addition, KRAs and KROs are limited to the recovery of escrowed keys. KRAs and KROs shall not perform any of the trusted role duties associated with the installation, initial set up, configuration and ongoing maintenance of the KED, including audit log review.

No individual in a trusted role 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, KRS and CSA shall be identified and assigned to trusted roles per Section 5.2.1.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to a background investigation. Personnel appointed to trusted roles (including CA trusted roles, KRS trusted roles, CSA trusted roles, and RA role) shall:

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

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

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

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

Each person filling a trusted role shall satisfy at least one of the following requirements:

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

For RAs and personnel appointed to trusted roles for the CSAs, in addition to the above, the person may be a citizen of the country where the RA or CSA function is located.

5.3.2 Background Check Procedures

All persons filling trusted roles (including the CA and RA systems' trusted roles, KRS trusted roles, CSA trusted roles, and RA role), shall have completed a favorable background investigation. The scope of the investigation shall include checking the following areas covering the past five years:

- Employment[4];
- Education (Regardless of the date of award, the highest educational degree shall be verified);

---

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

- Place of residence (past 3 years); and
- Law Enforcement.

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with United States Executive Order 12968 August 1995, or equivalent.

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

Background check procedures shall be described in the CertPS.

A favorable national agency check or security clearance that is based on a five-year background investigation meets the requirements of this section. For example, a successfully adjudicated United States National Agency Check with Written Inquires (NACI) or United States National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the requirements of this section, as is a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by ITAR – 22 CFR 120.32.

If a formal clearance or other check is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance or other check. Otherwise, the background check shall be refreshed every 10 years.

In circumstances where an interim clearance used to satisfy background check requirements is later found unfavorable, all certificates issued while the person had a trusted role shall be re-evaluated and possibly revoked at the discretion of the LM PMA.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of a CA, KRS, CSA or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/KRS/CSA/RA security principles and mechanisms;
- All PKI software versions in use on the CA and KRS system, including the DDS (if applicable);
- All PKI duties that personnel are expected to perform;
- Disaster recovery and business continuity procedures;
- Stipulations of the applicable CP and CertPS

In addition, KRAs and KROs shall be trained in the organizational policy relating to release of recovered escrowed keys and the information associated with such a recovery.

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

5.3.4 Retraining Frequency and Requirements

All personnel performing duties with respect to the operation of a CA, RA, KED, DDS, CSA, RA Workstation, or a KRA Workstation shall be aware of changes in the CA, RA, KED, DDS, CSA, or KRA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples

of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

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

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

5.3.6 Sanctions for Unauthorized Actions

Lockheed Martin shall take appropriate administrative and disciplinary actions against personnel who violate this certificate policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to CA, KED, DDS, CSA, KRS or RA operations shall meet applicable requirements as set forth in Section 5.3.

5.3.8 Documentation Supplied To Personnel

The CP, CertPS, and any relevant complementary documents, such as statutes, policies and contracts shall be made available to all trusted role personnel. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, KED, CSAs, RAs, Key Recovery Workstations and Administrative Workstations. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.

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

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

A statistically significant sample of KED audit records pertaining to successful key recoveries shall be reconciled against the KRA audit logs and self-recovery requests. All KED audit records of unsuccessful key recoveries shall be analyzed to determine the cause and to ensure that the Key Escrow and Recovery system is operating correctly and securely.

In addition, the event log of the Administration Workstation shall be reconciled with the event log of the corresponding CA, KED, DDS, CSA, or RA component when the Administration Workstation is used to administer said component.

The Audit Administrator shall explain all significant events in an audit log summary. Actions taken as a result of these reviews shall be documented.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA, KED, DDS, CSA, Administration Workstations (AW), and RA and KRA operating systems and the CA, KED, DDS, CSA, RA and KRA applications required by this CP shall be enabled during installation and remain enabled during operation. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- Location of the event (system affected or physical location),
- Source of the event,
- Success or failure where appropriate,
- The identity of any entity, object and/or operator associated with the event.

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

The assignment of an individual to a trusted role and removal of an individual from a trusted role are auditable events and shall include the name of the authorizing official.

In addition, and where applicable, KRAs shall monitor KRO activity for patterns of potentially anomalous behavior and initiate inquiries or investigations as appropriate.

The following events shall be audited:

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

Auditable Event	CA	KED	CSA	KRA	RA	DDS	AW
SECURITY AUDIT							
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X	X	X	X

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

Auditable Event	CA	KED	CSA	KRA	RA	DDS	AW
PRIVATE AND SECRET KEY EXPORT							
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X	X	X
CERTIFICATE REGISTRATION							
All records related to certificate request authorization, approval and signing	X	N/A	N/A	N/A	X	N/A	N/A
CERTIFICATE REVOCATION							
All records related to certificate revocation request authorization, approval and execution	X	N/A	N/A	N/A	X	N/A	N/A
CERTIFICATE STATUS CHANGE APPROVAL							
All records related to certificate status change request authorization, approval and execution	X	N/A	N/A	N/A	N/A	N/A	N/A
PKI COMPONENT CONFIGURATION							
Any security-relevant changes to the configuration of the Component	X	X	X	X	X	X	X
ACCOUNT ADMINISTRATION							
Roles and users are added or deleted	X	X	X	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT							
All changes to the certificate profile	X	N/A	N/A	N/A	N/A	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT							
All changes to the CSA profile (e.g. OCSP profile)	N/A	N/A	X	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT							
All changes to the certificate revocation list profile	X	N/A	N/A	N/A	N/A	N/A	N/A
MISCELLANEOUS							
Appointment of an individual to or removal from a Trusted Role	X	X	X	X	X	X	X

Auditable Event	CA	KED	CSA	KRA	RA	DDS	AW
Designation of personnel for multiparty control	X	X	-	X	N/A	X	X
Installation of the Operating System	X	X	X	X	X	X	X
Installation of the PKI Application	X	X	X	X	X	X	N/A
Installation of hardware cryptographic modules	X	X	X	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X	X	X	X
Destruction of cryptographic modules	X	X	X	X	X	X	X
System Startup	X	X	X	X	X	X	X
Logon attempts to PKI Application	X	X	X	X	X	X	X
Receipt of hardware / software	X	X	X	X	X	X	X
Attempts to set passwords	X	X	X	X	X	X	X
Attempts to modify passwords	X	X	X	X	X	X	X
Back up of the internal CA database	X	-	-	-	-	-	N/A
Restoration from back up of the internal CA database	X	-	-	-	-	-	N/A
Critical file manipulation (e.g., creation, renaming, moving)	X	X	-	X	-	X	N/A
Posting of any material to a repository	X	-	-	-	-	-	N/A
Access to the internal CA/KED database	X	X	X	X	-	X	N/A
All certificate compromise notification requests	X	N/A	N/A	N/A	X	X	N/A
Loading tokens with certificates	X	X	N/A	X	X	X	N/A
Shipment of tokens and receipt of tokens from/by the components that contain key material or that allow access to key material	X	X	N/A	X	X	X	N/A
Any action taken (e.g., authentication, authorization, recovery, and delivery) in response to a key recovery request	-	X	-	X	X	X	-

Auditable Event	CA	KED	CSA	KRA	RA	DDS	AW
Zeroizing and Destroying Tokens	X	X	N/A	X	X	X	N/A
Re-key of the Component	X	X	X	X	X	X	X
CONFIGURATION CHANGES							
Hardware	X	X	X	X	-	X	X
Software	X	X	X	X	X	X	X
Operating System	X	X	X	X	X	X	X
Patches	X	X	X	X	X	X	X
Security Profiles	X	X	X	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY							
Personnel Access to room housing Component	X	X	-	X	-	X	X
Access to the Component	X	X	X	X	-	X	X
Known or suspected violations of physical security	X	X	X	X	X	X	X
ANOMALIES							
Software error conditions	X	X	X	X	X	X	X
Software check integrity failures	X	X	X	X	X	X	X
Equipment failure	X	X	-	X	-	X	-
Electrical power outages	X	X	-	X	-	X	-
Uninterruptible Power Supply failure	X	X	-	-	-	X	-
Obvious and significant network service or access failures	X	X	-	X	-	X	-
Violations of Certificate Policy	X	X	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X	X	X
Resetting Operating System clock	X	X	X	X	X	X	X

Table 5.4.1-1 Auditable Events

5.4.2 Frequency of Processing Audit Logs

Audit logs shall be reviewed at least monthly, unless the CA is off-line, in which case the off-line CA's audit logs shall be reviewed when the system is activated or every 30 days, whichever is later.

5.4.3 Retention Period for Audit Logs

Audit logs shall be retained onsite until reviewed.

5.4.4 Protection of Audit Logs

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

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

For the CA, KED, DDS, CSA and the Administration Workstations, the Audit Administrator shall be the only person managing the audit log (e.g., collect, review, backup, rotate, delete, etc.). For the RA and KRA, a System Administrator other than the RA or KRA shall be responsible for managing the audit log. Note that a valid, trusted service account may be utilized to perform log backups automatically as needed.

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

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

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least once monthly, unless the CA is offline, in which case audit logs and audit summaries shall be backed up when the system is activated or every 30 days, whichever is later. A copy of the audit log shall be sent off-site in accordance with the CertPS.

5.4.6 Audit Collection System (internal vs. external)

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

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

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

If an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, the associated operations shall be suspended until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

CAs shall perform routine vulnerability assessments of the security controls described in this CP.

5.5 Records Archival

5.5.1 Types of Records Archived

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

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

Data To Be Archived	CA	KED	CSA	KRA	DDS	RA
Certification Practice Statement	X	X	X	X	X	X
Certificate Policy	X	X	X	X	X	X
Contractual obligations	X	X	X	X	X	X
System and equipment configuration	X	X	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X	X	X
All records related to certificate request, authorization, approval and signing	X	-	-	-	-	X
All records related to recovery of an escrowed key	-	X	-	X	X	-
All records related to certificate status changes (e.g., revocation, suspension, or restoration)	X	-	-	-	-	X

Data To Be Archived	CA	KED	CSA	KRA	DDS	RA
All records specific to the assignment of an individual to or removal from a trusted role	X	X	X	X	-	X
All records specific to the qualification, appointment, or removal of individuals as Trusted Agents	X	-	-	-	-	X
Certificate holder identity authentication data as per section 3.2.3	X	X	N/A	X	-	X
Documentation of receipt and acceptance of certificates, including Certificate Holder Agreements	X	-	N/A	-	-	X
Documentation of receipt of Tokens	X	X	N/A	X	-	X
All certificates issued or published	X	-	N/A	-	-	N/A
Record of Component CA Re-key	X	X	X	X	-	X
All Audit Logs	X	X	X	X	X	X
Other data or applications to verify archive contents	X	X	X	X	X	X
Documentation required by compliance auditors	X	X	X	X	X	X
Compliance Audit Reports	X	X	X	X	X	X

5.5.2 Retention Period for Archive

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

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Alternatively, Lockheed Martin may retain data using procedures detailed within the records retention policies it publishes in its Corporate Command Media. Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to write to, modify, or delete the archive. For the CA, KED, DDS and CSA, the authorized individuals are audit administrators. For the RA and KRA, authorized individuals are someone other than the RA or KRA. The contents of the archive shall not be released except as determined by the PMA or as required by law. Records of individual transactions may be released upon request of any certificate holders involved in the transaction or their legally recognized agents.

Archive media shall be stored in a secure storage facility separate from the PKI components (CA, KED, DDS, CSA, KRA or RA) with physical and procedural security controls equivalent or better than those of the PKI. Deletion of archive records is not permitted under any circumstances prior to the end of the required retention period.

5.5.4 Archive Backup Procedures

Not Applicable.

5.5.5 Requirements for Time-Stamping of Records

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

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

5.5.6 Archive Collection System (internal or external)

The archive collection system may be internal or external and is identified in the CertPS .

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 CertPS.

5.6 Key Changeover

As a CA approaches the end of its validity period, planning shall be initiated to ensure a smooth transition to a new CA, unless it is Lockheed Martin's intention to cease certificate production.

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

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

	Lifetime	
Certificate type	Private Key	Certificate
Self-signed Offline Root CA	20 years	20 years
Signing CA	10 years	10 years*
Cross certificates issued to a Bridge CA	3 years	3 years
Certificate holder Identity or Signature	3 years	3 years

Certificate holder Encryption	Unrestricted	3 years
Code Signer	3 years	8 years
OCSP Responder	3 years	120 days
SCVP Server	3 years	3 years
Server	3 years	3 years

*For Intermediate and Signing CAs with at least 3072 bit key length, certificate lifetime may be extended to 13 years.

No CA, including a Bridge CA, shall have a private key that is valid for longer than 20 years. Cross certificates shall not be valid for more than 3 years.

CAs must not issue certificate holder certificates that extend beyond the expiration date of their own certificates and public keys.

Notwithstanding the above table, in all cases the CA private key may be used to sign OCSP certificates and CRLs until the CA certificate expires.

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

5.7 Compromise and Disaster Recovery

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

5.7.1 Incident and Compromise Handling Procedures

Lockheed Martin shall have a formal disaster recovery plan.

If the Lockheed Martin PKI 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, KED, DDS or CSA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA, KED, DDS or CSA needs to be rebuilt, only some certificates need to be revoked, and/or the CA, KED, DDS or CSA key needs to be declared compromised. If it is determined that an incident has occurred with the potential to affect the operations and/or security environments, the members of the LM PMA, applicable cross-certified PKIs as well as the CBCA shall be notified within 24 hours of determination and provided a preliminary remediation analysis.

Once the incident has been resolved, the CA owner shall notify the LM PMA, applicable cross-certified PKIs as well as the CBCA. The notification shall provide detailed measures taken to remediate the incident and include the following:

- Which CA components were affected by the incident
- The CA's interpretation of the incident
- Who is impacted by the incident

- When the incident was discovered
- A statement that the incident has been fully remediated.

The Lockheed Martin Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CertPS.

5.7.2 Computing Resources, Software, and/or Data Corruption

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

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued certificates by the CA shall be securely[5] notified immediately. This will allow other CAs to protect their certificate holders' interests as Relying Parties.

If the ability to revoke certificates is inoperative or damaged, the CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CertPS. If the CA's revocation capability cannot be established in a reasonable timeframe, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all certificate holders that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

5.7.3.1 CA, CSA and RA Private Key Compromise Procedures

If CA's signature keys are compromised, lost, or suspected of compromise:

1. The CA shall request revocation of any certificates issued to the compromised CA immediately;
2. A new CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CertPS;
3. New CA certificates shall be requested in accordance with the initial registration process described 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 remaining the same as in original certificates; and
5. If the CA is a Root CA, the new self-signed certificate shall be distributed to Certificate Holders using secure means.

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

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

If a CSA key is compromised, all certificates issued to the CSA shall be revoked, if applicable. The CSA shall generate a new key pair and request new certificate(s), if applicable. If the CSA is a trust anchor, the relying parties will be provided the new trust anchor in a secure manner (so that the trust anchor integrity is maintained) to replace the compromised trust anchor.

If RA signature keys are compromised, lost, or suspected of compromise:

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

5.7.3.2 KRS Private Key Compromise Procedures

In the event that a KED or DDS is compromised or is suspected to be compromised, the Lockheed Martin PMA shall be notified. The Lockheed Martin PMA shall be granted sufficient access to information to determine the extent of the compromise. The Lockheed Martin PMA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED.

If the KRA or KRO certificate is compromised, lost, or suspected of compromise:

1. The KRA or KRO certificate shall be revoked immediately;
2. A new key pair shall be generated in accordance with procedures set forth in the applicable CertPS;
3. A new certificate shall be requested in accordance with the initial registration process in Section 3.2.
4. All key recovery actions undertaken by the KRA or KRO since the date of the suspected compromise shall be reviewed to determine whether the escrowed keys may have been exposed during the recovery process;
5. The certificates associated with the potentially exposed escrowed keys shall be revoked, according to procedures specified in Section 4.9.3, and the Certificate Holder shall be notified of the revocation.

   Note: It is recognized that this will constitute implicit notification to the Certificate Holder of key recovery.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request revocation of its certificates. Further, the CA shall re-establish operations as quickly as possible by following the procedures for CA key loss or compromise detailed in Section 5.7.3 above.

5.8 CA, CSA, KED, DDS and RA Termination

In the event of a CA termination, the LM PKI will provide notice to all cross-certified CAs.

Prior to the termination of a CA, the CA shall request revocation of all certificates issued to it.

In addition:

- The CA, CSA, KED, DDS KRA and RA shall archive all audit logs and other records prior to termination.
- The CA, CSA, KED, DDS, KRA and RA shall destroy all private keys upon termination.
- The CA, CSA, KED, DDS, KRA and RA audit-archive records shall be transferred to an appropriate authority such as the LM PMA.
- If a Root CA is terminated, Lockheed Martin shall use secure means to notify the Certificate Holders to delete all trust anchors representing the terminated CA.

Whenever possible, notification of termination will be provided at least two weeks prior to the CA termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

Entity	FIPS 140 Level	Hardware or Software	Key Storage Restricted To The Module on Which The Key Was Generated
CA	3	Hardware	Yes
KED	3	Hardware	Yes
DDS	3	Hardware	Yes
RA/KRA/KO	2	Hardware	Yes
OCSP Responder	2	Hardware	Yes
Code Signing	2	Hardware	Yes

End Entity Signature or Authentication (medium-software)	1	Software	No Requirement
End Entity Encryption (medium-software)	1	Software	No Requirement
End Entity Signature or Authentication (medium-hardware)	2	Hardware	Yes
End Entity Encryption (medium-hardware)	2	Hardware	No Requirement
Server (medium-software)	1	Software	No Requirement
Server (medium-hardware)	2	Hardware	Yes

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

Random numbers for medium-hardware and medium-device-hardware assurance level Certificate Holder 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 from acting as the key escrow module.

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

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

6.1.2 Private Key Delivery to Certificate holder

A CA shall generate its own key pair and therefore does not need private key delivery.

If certificate holders 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 Certificate holder, then the private key shall be delivered securely to the Certificate holder. 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 Certificate holder shall not retain any copy of the key after delivery of the private signing key to the Certificate holder.
- The private key shall be protected from activation, compromise, or modification during the delivery process.
- The Certificate holder 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 Certificate holders.
    - For hardware modules, accountability for the location and state of the module shall be maintained until the Certificate holder 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 being delivered. Activation data shall be delivered using a separate secure channel.

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

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the certificate holders 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 a trust anchor include but are not limited to:

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

6.1.5 Key Sizes

If the LM PMA determines that the security of a particular permitted algorithm may be compromised**,** it may require the CAs to revoke the affected certificates.

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

Usage	**Public Key Algorithm**	**Sunset Date**
Signature	2048-bit RSA, 256-bit ECDSA in prime field, or 283-bit ECDSA in binary field	12/31/2030
	3072- or 4096-bit RSA, 256-bit ECDSA in prime field, or 283-bit ECDSA in binary field	12/31/2035
	ML-DSA-44 (Category 2) ML-DSA-65 (Category 3) ML-DSA-87 (Category 5)	No stipulation
Encryption	2048-bit RSA, 256-bit ECDH in prime field, or 283-bit ECDH in binary field	12/31/2030
	3072- or 4096-bit RSA, 256-bit ECDH in prime field, or 283-bit ECDH in binary field	12/31/2035
	ML-KEM-512 (128 bit) ML-KEM-768 (192 bit) ML-KEM-1024 (256 bit)	No stipulation

All data encryption (including network protocols) used by or in connection with PKI components for administration, communications, and protection of keys or other sensitive data shall use the Advanced Encryption Standard (AES) symmetric algorithm with a minimum key size of 128-bits.

All certificates (excluding self-signed certificates), CRLs, and OCSP Responses shall use the following hashing algorithms for the time periods indicated:

	Issued before 12/31/2030	**Issued after 12/31/2030**
Hashing Algorithm for Certificates, CRLs and OCSP Responses	SHA-256 or, SHA-384	SHA-256, SHA-384 or, SHA-512

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

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

The use of a specific key is determined by the key usage and extended key usage extensions in the X.509 certificate.

- Certificates to be used for authentication shall set the digitalSignature bit only.
- Certificates to be used by human Certificate Holders for digital signatures shall set the *digitalSignature* and *nonRepudiation* bits.
- Certificates that have the *nonRepudiation* bit set, shall not have *keyEncipherment* bit or *keyAgreement* bit set.
- Certificates to be used for encryption shall set the *keyEncipherment* bit.
- Certificates to be used for key agreement shall set the *keyAgreement* bit.
- CA certificates shall set cRLSign and keyCertSign bits.

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

Public keys that are bound into human Certificate Holder certificates shall be certified for use in signing or encrypting, but not both.

Device Certificate Holder certificates that provide authenticated connections using key management certificates may set both the *digitalSignature* and *keyEncipherment* bits. With the exception of OCSP Responder certificates, device certificates must not assert the *nonRepudiation* bit.

For End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}.

The extended key usage shall meet the requirements stated in Section 10.12. Extended Key Usage values shall be consistent with key usage bits asserted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS 140, *Security Requirements for Cryptographic Modules*. The LM PMA may determine that other comparable validation, certification, or verification standards are also sufficient. These standards will be published by the LM PMA. Cryptographic modules shall be validated to the FIPS 140 level identified in

section 6.1.1 or equivalent. The LM PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CA.

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

6.2.2 Private Key Multi-Person Control

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

6.2.3 Private Key Escrow

Under no circumstances shall signature keys be escrowed by a third-party.

For human Certificate Holders, private keys used for decryption shall be escrowed.

For Device Certificate Holder private keys used for decryption, escrow is mandatory unless the data protected by these keys will never require recovery. This escrow shall take place prior to the generation of the corresponding certificates.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as used to generate and protect the original signature key. A single backup copy of the signature key shall be stored at or near the CA location. A second backup copy shall be kept at the CA backup location. Procedures for CA private signature key backup shall be included in the appropriate CertPS and shall meet the multiparty control requirement of Section 5.2.2.

6.2.4.2 Backup of KED Private Decryption Key

The KED key shall be backed up as necessary to provide secure continuity of key recovery operations. The backup keys shall only be created, stored, and restored under two-person control. The process of restoring the backup KED key shall maintain two party control throughout and shall meet the multiparty control requirement in Section 5.2.2.

6.2.4.3 Backup of Certificate holder Private Signature Key

Certificate holder private signature keys whose corresponding public key is contained in a certificate asserting medium-software may be backed up or copied but the backup must be held in the Certificate Holder's control. Storage must ensure security controls consistent with the protection provided by the Certificate holder's cryptographic module.

Device private signature keys whose corresponding public key is contained in a certificate asserting medium-device-software may be backed up or copied but must be held in the control of the device's human sponsor or other authorized administrator.

Certificate holder private signature keys whose corresponding public key is contained in a certificate asserting medium-hardware shall not be backed up or copied.

6.2.4.4 CSA Private Key Backup

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

6.2.5 Private Key Archival

Private signature keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA, KED, DDS and CSA private keys shall be generated by and remain in an approved cryptographic module. The keys may be backed up in accordance with Section 6.2.4.

If any private key is transported from one cryptographic module to another, the private key shall be protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported.

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

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

6.2.9 Methods of Deactivating Private Key

After use, a Certificate Holder's cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CertPS. Activated cryptographic modules shall not be left unattended or otherwise open to unauthorized access. Removable cryptographic modules shall be protected when not in use.

CA, CSA, KED and DDS hardware cryptographic modules shall be removed and stored in a secure container when not in use. If a cryptographic module contains a complete (versus split) key for activating CA, CMS, KED, or DDS keys, all storage procedures and mechanisms for that module shall require two-person control.

6.2.10 Method of Destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be accomplished by overwriting the data. For hardware cryptographic modules, this will usually require executing a "zeroize" command.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods/Key Usage Periods

See Section 5.6.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For Medium Assurance Hardware Device Certificates and Medium Assurance Software Device Certificates, private keys may be activated without entry of activation data.

For all other policies governed by this CP, the activation data used to unlock private keys, in conjunction with any other access control procedure, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Certificate holder activation data may be user selected. For CAs, activation data shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key or upon appointment of new Administrator or Operator trusted roles.

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, memorized, or contained within an organizationally approved device or software tool (e.g., password manager) that leverages encryption commensurate with the bit-strength of the key it activates. If written down, activation data 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. In all cases, 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 Lockheed Martin CertPS.

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.

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

In addition, the KRS shall be provided with residual information protection by the underlying operating system.

When CA and KRS equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall,

where possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The computer system shall be configured with the minimum of the required accounts and network services.

6.5.2 Computer Security Rating

Not applicable.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA, KED, DDS, KRA and CSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology.
- Where open-source software has been utilized, security requirements shall be achieved through software verification & validation and structured development lifecycle management.
- Procured hardware and software 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).
- Specially developed hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing PKI activities. There shall be no other applications: hardware devices, network connections, or component software installed which is not part of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Applications required to perform PKI operations shall be obtained from sources authorized by local policy. 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 the CA, KED, DDS, CSA, Administration Workstations, KRA and RA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism to periodically verify the integrity of the software and to detect unauthorized modification to the CA, KED, DDS and CSA software or configuration. The CA, KED, DDS and CSA software, when first loaded, shall be verified as being that supplied by the vendor, with no modifications, and as the version intended for use.

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

In addition, only applications required to perform the organization's mission shall be loaded on the Administration Workstations, KRA, KRO or RA workstations, and all such software shall be obtained from sources authorized by local policy.

6.6.3 Life Cycle Security Controls

Not applicable.

6.7 Network Security Controls

CAs, KEDs, DDSs, CSAs, Administration Workstations, KRAs and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls, and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

If the Administration Workstation is located outside the security perimeter of the CA, KED, DDS and CSA, it shall access the PKI Enclave using site-to-site VPN. The VPN shall use FIPS approved cryptography commensurate with the cryptographic strength of certificates issued by the PKI being administered. The VPN shall be configured for mutual authentication, encryption and integrity. If mutual authentication is shared secret based, the shared secret shall be changed at least annually, shall be randomly generated, and shall have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered. Alternatively, when the Administration Workstation is located inside the security perimeter of the CA, KED, DDS and CSA, and protected by the boundary controls of the PKI Enclave, appropriate techniques shall be used for mutual authentication of the PKI components and mutual authentication of traffic flowing among them.

Any boundary control devices used to protect the network on which the PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Remote access shall be mediated by a bastion host or “jump server” (i.e. a machine that presents a limited interface for interaction). All network activity to the PKI components (e.g.

CA, KED, DDS and/or CSA) shall be initiated from the bastion host. The bastion host is considered part of the CA, KED, DDS and/or CSA and shall meet the security requirements for these components. A remote workstation or user shall perform mutual authentication with the bastion host using strong authentication (e.g., PKI credential) commensurate with the cryptographic strength of certificates issued by the PKI being administered. Cryptographic material derived from the authentication shall be used to protect the communication with the bastion host. (Note: client-authenticated TLS, SSH and IPSEC are examples of protocols that meet this requirement.) In addition, the user shall authenticate to the PKI component being administered via the bastion host. In other words, authentication to the bastion host does not alleviate the need to authenticate to the PKI component(s) being administered.

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

Root CAs and their internal PKI repositories shall be offline.

6.8 Time Stamping

All CA and CSA components shall regularly synchronize with a time service such as the National Institute of Standards and Technology (NIST) Atomic Clock or the 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 Certificate holder's Certificate
- Revocation of a Certificate holder's Certificate
- Posting of CRL updates
- OCSP or other CSA responses

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Section 10 contains the certificate profiles.

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

CA certificates shall not include critical private extensions.

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

Issuer CA and Certificate Holder certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 Algorithm Object Identifiers

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha384(3)}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha512(4)}

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

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 RFC 5280. Subject and issuer fields shall include attributes as detailed in the table below.

Issuer and Subject Name Form (CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities” or similar text
	Required	O	1	Issuer name, e.g., “O=XYZ Inc”
	Required	C	1	Country name, e.g., “C=US”
2	Recommended	CN	0…1	Descriptive name for CA, e.g., “CN=XYZ Inc CA”
	Optional	OU	0…N	As needed
	Recommended	OU	0…1	“Certification Authorities”, or similar text
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc”
	Optional	C	0…1	Country name, e.g., “C=US”
	Required	DC	1	Domain name, e.g., “DC=xyzinc”
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc.

Subject Name Form (Non-CAs)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Required	O	1	Issuer name, e.g., “O=XYZ Inc” within an authorized name space
	Required	C	1	Country name, e.g., “C=US” within an authorized name space
2	Required	See Content description	1…N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, etc.
	Optional	OU	0…N	As needed
	Optional	O	0…1	Issuer name, e.g., “O=XYZ Inc” within an authorized name space

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
	Required	DC	1	Domain name, e.g., “DC=xyzinc” within an authorized name space
	Required	DC	1…N	Domain root label(s), e.g., “DC=com” or, “DC=com, DC=au”, etc. within an authorized name space

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

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

7.1.6 Certificate Policy Object Identifier

With the exception of self-signed Root CA certificates, all CA and Certificate Holder certificates shall contain at least one certificate policy OID listed in Section 1.2 of this document.

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

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

7.1.7 Usage of Policy Constraints Extension

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

The LM Signing CA may, optionally, assert the policy constraints extension to inhibit policy mapping by relying parties and/or to require explicit policy.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The certificate policies extension shall not be marked critical.

7.1.10 Inhibit Any Policy Extension

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

7.2 CRL Profile

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

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

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

7.3.1 Version Number

The version number for requests and responses shall be v1.

7.3.2 OCSP Extensions

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Lockheed Martin Policy Management Authority, working with the Operational Authority, shall have a compliance audit mechanism in place to ensure that the requirements applicable to AGREEMENTs, this CP, and the related CertPS are being implemented and enforced.

8.1 Frequency or Circumstances of Assessments

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

8.2 Identity and Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor shall represent a firm, which is independent from Lockheed Martin, or it shall be sufficiently organizationally separated from the Lockheed Martin Enterprise PKI as to provide an unbiased, independent evaluation. An example of the latter situation may be an audit department within Lockheed Martin provided it can demonstrate organizational separation and independence. To further ensure independence and objectivity, the compliance auditor may not have served Lockheed Martin in developing or maintaining Lockheed Martin's PKI Facility, associated IT and network systems, or certificate practices statement. The LM PMA Chair shall determine whether a compliance auditor meets this requirement.

In the event the Lockheed Martin Enterprise PKI chooses to engage compliance auditor services internal to Lockheed Martin, it shall undergo an audit from an external third-party audit firm every third year, at a minimum.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP and the CertPS as well as any applicable AGREEMENT. All aspects of the operation of the LM PKI shall be subject to compliance audit inspections.

The compliance audit must include an assessment of the CertPS against this CP, to determine that the CertPS adequately addresses and implements the requirements of the CP.

8.5 Actions Taken as a Result of Deficiency

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

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the LM PMA Chair of the discrepancy;
- The LM PMA Chair shall notify the CertiPath and/or TSCP (or other LM PMA-Approved Bridge Authority's) PMA of the discrepancy and communicate the discrepancy mitigation plan;
- 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 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 LM PMA may decide to halt temporarily operation of the CA, to revoke a certificate issued by the CA, or to take other actions it deems appropriate. The LM PMA shall develop procedures for making and implementing such determinations.

8.6 Communication of Results

An Audit Compliance Report package, including identification of corrective measures taken or being taken by the CA, shall be provided to the LM PMA as set forth in Section 8.1. This package shall be prepared in accordance with the "Compliance Audit Reference Documents" and must include an assertion from the LM PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CertPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

In addition, for cross-certified PKIs, the Audit Compliance Report package, including identification of corrective measures taken or being taken by the CA, shall be provided to the CertiPath and/or TSCP (or other LM PMA-Approved Bridge Authority's) PMA.

Practice Note: The different components of the Infrastructure may be audited separately. In these cases, the Compliance Audit Package will contain multiple audit reports, one for each separately audited component.

---

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Not applicable

9.1.1 Certificate Issuance and Renewal Fees

Not applicable

9.1.2 Certificate Access Fees

Not applicable

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

Organizations acting as relying parties shall determine the financial risk, if any; they undertake when accepting certificates to consummate any transaction. Acceptance of Lockheed Martin 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 statutory imposed constraints.

9.2.1 Insurance Coverage

Lockheed Martin maintains reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants, as those entities are described in Section 1.3 of this CP.

9.2.2 Other Assets

Lockheed Martin shall maintain sufficient financial resources to maintain operations and to fulfill duties.

9.2.3 Insurance or Warranty Coverage for Relying Parties

Lockheed Martin does not offer protection from risk to relying parties beyond the protections specifically stated in this CP.

9.3 Confidentiality of Business Information

Lockheed Martin shall maintain the confidentiality of properly labeled proprietary information that is clearly marked or labeled as confidential, or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care and security as it treats its own confidential information.

When key recovery is requested as part of an investigation or court order, information concerning the request shall be protected from unauthorized disclosure.

9.4 Privacy of Personal Information/Personal Data

Lockheed Martin shall collect, store, process, and control access and disclosure of Personal Information/Personal Data (PI/PD) in accordance with applicable Lockheed Martin Corporate Policy, which shall be available to employees and non-employees with a Lockheed Martin Smart Card supplying PI/PD. The storage of PI/PD will be limited to the minimum necessary to validate the identity of the Certificate Holder or Key Recovery Requestor. This may include attributes that correlate identity evidence to authoritative sources. The Registration Authority (RA) will provide explicit notice to the Certificate Holder regarding the purpose for storing a record of the PI/PD necessary for identity proofing and the consequences for not providing the information. PI/PD stored for identity proofing purposes will only be used for proofing-related business purposes.

9.5 Intellectual Property Rights

The Lockheed Martin Operational Authority shall not knowingly violate any intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

Lockheed Martin retains all Intellectual Property Rights in and to the certificates and revocation information it issues.

9.5.2 Property Rights in the CertPS

All Intellectual Property Rights in this CP and Lockheed Martin's CertPS are owned by Lockheed Martin and/or its licensors.

9.5.3 Property Rights in Names

As between Lockheed Martin and a Certificate Applicant, the Certificate Applicant retains all rights, if any, in any trademark, service mark, or trade name of the Certificate Applicant.

9.5.4 Property Rights in Keys

Key pairs bound to Certificates of Lockheed Martin CAs and Certificate holders are the property of the Lockheed Martin CAs and Certificate holders respectively.

Lockheed Martin's root public keys and the root Certificates containing them, including all signing CA public keys and self-signed Certificates, are the property of Lockheed Martin.

9.6 Representations and Warranties

Representations and warranties contained in agreements between Lockheed Martin and other involved parties are contained in the following documents:

- Policy Mapping Agreement between Lockheed Martin and CertiPath
- Master Services Agreement between Lockheed Martin and CertiPath
- Applicable Memorandums of Agreement.

The above-listed documents may contain additional and/or supplemental representations and warranties between the parties.

9.6.1 CA Representations and Warranties

Lockheed Martin certificates are issued at the sole discretion of the LM PMA. In the event the Lockheed Martin US Signing Certification Authority issues a cross-certificate to a non-Lockheed Martin CA, it does so for the convenience of Lockheed Martin.

Lockheed Martin represents and warrants that, to its knowledge:

- There are no material misrepresentations of fact in the cross-certificates known to or originating from the Lockheed Martin PMA or the Lockheed Martin Enterprise PKI's OA,
- There are no errors in the information in the cross-certificate that were introduced by Lockheed Martin as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Certificates meet all material requirements of this CP, and Revocation services and use of a repository conform to the CertPS in all material aspects.
- The CA signing key is protected and that no unauthorized person has ever had access to the private key,
- All representations made, with respect to the CA in the applicable AGREEMENTS are true and accurate, to the best of its knowledge
- Where applicable, all information supplied by the Certificate holders and CA subjects in connection with, and/or contained in the Certificate is true,
- The Certificates are being used by the CA exclusively for authorized and legal purposes, consistent with this CP or CertPS, to the best of its knowledge.

The applicable contractual agreements may include additional representations and warranties.

9.6.2 RA, KRA and KRO Representations and Warranties

Registration Authorities shall represent and warrant that identity verification is performed in accordance with Section 3 of the applicable certificate policy.

KRAs shall:

- represent and warrant that Certificate Holder's escrowed keys shall be released only for properly authenticated and authorized requests.

- validate the authorization of the KRO to act on behalf of the Certificate Holder whose key recovery has been requested.
- communicate knowledge of a recovery process only to the KROs and Requestor involved in the key recovery, and to those other individuals with a need to know as determined by organizational policy.
- protect Certificate Holder's escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- protect recovered keys from compromise.
- protect all information, including the KRA's own key(s) used to recover Certificate Holder's escrowed keys.

In the event the Key Recovery Requestor is someone other than the Certificate Holder (i.e., Third-party Requestor), the KRA or KRO shall validate the Key Recovery Requestor's authority to request the Certificate Holder's private key. In addition, KROs shall

- accurately represent themselves when requesting key recovery services.
- validate the identity of the requestor seeking a key recovery
- communicate knowledge of a recovery process only to the KRAs and the Key Recovery Requestor, and to those other individuals with a need to know as determined by organizational policy.
- protect all information, including the KRO's own key(s) used to request recovery of Certificate Holder's escrowed keys.
- retain records pertaining to recovery requests and disposition, including acknowledgment of receipt by the Key Recovery Requestor.

9.6.3 Certificate Holder

To obtain a certificate a Certificate Holder shall be required to sign a document, either before issuance or immediately following, requiring that the Certificate holder satisfy certain obligations including, but not limited to:

- Protection of the private key;
- Proper use of the certificate;
- Accurately represent themselves in all communications with the issuing PKI authorities;
- Abide by all export control restrictions;
- Acknowledge that any information contained within a certificate is not considered private; and
- Prompt notification to the appropriate CA upon suspicion of loss or compromise of its private key. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CertPS.

In signing the document described above, each Certificate Holder shall represent and warrant that:

- The data contained in any certificates issued to the Certificate Holder is accurate;
- The Certificate holder lawfully holds the private key corresponding to the public key identified in the Certificate Holder's certificate;
- The Certificate Holder will protect its private keys at all times, in accordance with this policy, as stipulated in the certificate acceptance agreements and local procedures; and
- The Certificate Holder will abide by all the terms, conditions, and restrictions levied on the use of private keys and certificates.

A PKI sponsor shall assume the Certificate Holder's obligations for devices.

9.6.4 Relying Party

Parties who rely upon the certificates issued under a policy defined in this document shall:

- use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- establish trust in the CA that issued the certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Affiliated Organizations

Not applicable

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 Third-party Key Recovery Requestors

Third-Party Key Recovery Requestors shall formally acknowledge and agree to the obligations described here:

- Request and use the Certificate Holder's escrowed keys only to recover data they are authorized to access.
- Protect Certificate Holder's recovered keys from compromise using a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls commensurate with the level of assurance of the keys being recovered.

- Destroy Certificate Holders' private keys when no longer needed (i.e., data has been recovered) in accordance with the process established in Section 6.2.10 of the associated CertPS.
- Accurately represent themselves during any key recovery operation.
- Protect information concerning each key recovery operation.
- Sign an acknowledgment of agreement to follow the law and Lockheed Martin's policies relating to protection and release of the recovered key. Such agreement shall include the following attestations:
    - Requestor has been accurately identified,
    - Requestor has truthfully described the reason(s) for the key recovery request,
    - Requestor has a legitimate and official need to obtain the requested key,
    - Requestor has received the recovered key,
    - Requestor shall use the recovered key only for the stated purposes,
    - Requestor shall protect the recovered key from unauthorized access and shall destroy the key or return it to Lockheed Martin when no longer needed,
    - Requestor is bound by applicable laws and regulations concerning the protection of the recovered key and any data recovered using the key.

9.6.6.2 Data Decryption Servers

Prior to the beginning of the operation of a DDS, the person acting as the PKI Sponsor for the DDS shall formally acknowledge and agree to the obligations described here, in accordance with the stipulations of the applicable CP:

- The DDS shall accurately identify and authenticate itself to a degree commensurate with the assurance level of the key being requested.
- The DDS shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect its own keys and recovered subscribers' keys.
- The DDS shall destroy subscribers' keys when no longer required (i.e., when the data has been recovered).
- The DDS shall request and use a subscriber's escrowed key(s) only upon receipt of a request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an email Server)

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Policy Mapping Agreements, cross-certificates Agreements, Memorandums of Agreement, and any other related agreements may contain

disclaimers of all warranties (other than any express warranties contained in such agreements or set forth in this CP).

TO THE EXTENT PERMITTED BY APPLICABLE LAW, LOCKHEED MARTIN CAs MAY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTIES, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CP.

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN LOCKHEED MARTIN AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS, (A) CERTIFICATES ISSUED BY LOCKHEED MARTIN ARE PROVIDED "AS IS", AND LOCKHEED MARTIN, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS, AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY AND COMPLETENESS OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY LOCKHEED MARTIN CERTIFICATES, ANY SERVICES PROVIDED BY LOCKHEED MARTIN, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 Limitations of Liabilities

The liability (and/or limitation thereof) of Lockheed Martin CAs with respect to its issued certificates shall be set forth in the applicable agreements.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LOCKHEED MARTIN BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL, AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS CP SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT.

9.9 Indemnities

9.9.1 Indemnification by cross-certified CAs

To the extent permitted by applicable law with respect to certificates issued by cross-certified CAs, cross-certified CAs are required to indemnify Lockheed Martin for:

- Falsehood or misrepresentation of fact by the cross-certified CA in the applicable contractual agreements.

- Failure by the cross-certified CA to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The cross-certified CA failure to protect the cross-certified CA private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the cross-certified CA private key, or
- The cross-certified CA use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable contractual agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, each Relying Party shall indemnify Lockheed Martin and its contractors, agents, assigns, employees, officers, and directors from and against any third party claims, liabilities, damages, costs, and expenses (including reasonable attorney's fees), relating to or arising out of the use of or reliance by the Relying Party on any certificates issued by Lockheed Martin, including, without limitation, for:

- The Relying Party's improper, illegal, or unauthorized use of a Certificate (including use of any expired, revoked, or unvalidated Certificate);
- The Relying Party's unreasonable reliance on a Certificate, given the circumstances, or,
- The Relying Party's use of a Certificate that asserts a "pass-through" policy OID as defined in Section 1.2 of this CP; or
- The Relying Party's failure to check the status of a Certificate on which it relies to determine if the Certificate is expired or revoked.

Any applicable contractual agreement between Lockheed Martin and a Relying Party may include additional indemnity obligations assumed by the Relying Party relating to or arising from its reliance upon the Lockheed Martin PKI.

9.10 Term and Termination

9.10.1 Term

This CP becomes effective upon ratification by the LM PMA and publication in the LM Repository. Amendments to this CP become effective upon ratification by the LM PMA and publication in the LM Repository.

9.10.2 Termination

This CP may be amended from time to time, it shall remain in force until replaced by a newer version or until terminated. Termination of this CP is at the discretion of the Lockheed Martin Policy Management Authority. For purposes of clarity, termination of any AGREEMENT shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the LM PMA.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, Lockheed Martin CAs operating under this policy are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. The following sections of this CP shall survive the termination or expiration of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13 -9.16.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, LM shall use commercially reasonable methods to communicate with cross-certified CAs, taking into account the criticality and subject matter of the communication.

Any planned change to the infrastructure of an LM CA that has the potential to affect cross-certified PKIs or a CBCA operational environment shall be communicated to the PMA of the cross-certified PKIs or CBCA at least two weeks prior to implementation, and any new CA certificates produced as a result of the change shall be provided to the cross-certified PKIs or CBCAs within 24 hours following implementation.

9.12 Amendments

9.12.1 Procedure for Amendment

The LM PMA reviews the CP and CertPS at least once every year. Additional reviews may be performed at any time at the discretion of the LM PMA.

If the LM PMA wishes to recommend amendments, including modifications or corrections, to the CP or CertPS, such amendments shall be circulated to appropriate parties identified by the LM PMA. Comments from such parties will be collected by the LM PMA in a fashion determined by the LM PMA.

After collection and incorporation of comments, the LM PMA shall make the necessary amendments. Following approval by the LM PMA, public notification of amendments shall be made.

Notwithstanding the foregoing, if the LM PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of LM, LM shall be entitled to make such amendments effective immediately upon publication in the Repository for on-line access.

9.12.2 Notification Mechanism and Period

Errors, updates, and anticipated changes to the CP and CertPS resulting from reviews are published online. In addition, changes are communicated to the LM PMA, including a description of the change.

This CP and all subsequent changes to it shall be made publicly available within thirty (30) days of approval.

9.12.3 Circumstances under Which OID Must be Changed

Certificate Policy OIDs shall be changed if the LM PMA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Lockheed Martin and Customers

Provisions for resolving disputes between Lockheed Martin and its Customers shall be set forth in the applicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

Except as otherwise agreed (e.g., under an agreement described in Section 9.13.1 above), any dispute under this CP shall be resolved by arbitration in accordance with the commercial rules (or international rules, if the other party to the dispute is a non-US entity) of the American Arbitration Association then in effect. The arbitration panel shall consist of one (1) neutral arbitrator if the amount in controversy is less than $10,000; otherwise the panel shall consist of three (3) neutral arbitrators, each an attorney with five (5) or more years of experience in computer and technology law and/or the primary area of law as to which the dispute relates. The arbitrator(s) shall have never been employed (either as an employee or as an independent consultant) by either of the Parties, or any parent, subsidiary, or affiliate thereof. The Parties shall have the right to take discovery of the other Party by any or all methods provided in the Federal Rules of Civil Procedure. The arbitrator(s) may upon request exclude from being used in the arbitration proceeding any evidence not made available to the other Party pursuant to a proper discovery request. The arbitrator(s) shall apply federal law of the United States and/or the law of the State of New York, and the arbitration proceeding shall be held in New York City, New York, USA or in such other location as is mutually agreed upon. The cost of the arbitration shall be borne equally by the Parties, unless the arbitrator(s) awards costs and attorneys fees to the prevailing Party. Notwithstanding the choice of law provision in this Agreement, the Federal Arbitration Act, except as modified herein, shall govern the interpretation and enforcement of this provision. All arbitration proceedings shall be conducted in English. Any claim, dispute, and controversy shall be arbitrated on an individual basis and not aggregated with the claims of any third party class action arbitration. The arbitrator(s) shall have no discretion to award punitive damages. Notwithstanding the foregoing dispute resolution procedures, either Party may apply to any court having jurisdiction to (i) enforce the agreement to arbitrate, (ii) seek provisional injunctive relief so as to maintain the status quo until the arbitration award is rendered or the dispute is otherwise resolved, or to otherwise prevent irreparable harm, (iii) avoid the expiration of any applicable limitation period, (iv) preserve a superior position with respect to creditors, or (v) challenge or vacate any final decision or award of the arbitration panel that does not comport with the express provisions of this CP.

9.14 Governing Law

Subject to any limits appearing in applicable law, the federal laws of the United States and/or the laws State of New York shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of New York. This choice of law is made to ensure uniform procedures and interpretation for all Lockheed Martin CAs, no matter where they are located.

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

9.15 Compliance With Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party. Such consent shall not be unreasonably withheld.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

Lockheed Martin shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of

equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action. LOCKHEED MARTIN HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO LOCKHEED MARTIN.

9.17 Other Provisions

None.

10 CERTIFICATE, CRL, AND OCSP FORMATS

This section contains the formats for the various PKI objects such as certificates, CRLs, and OCSP requests and responses.

Certificates and CRLs issued under a policy OID of this CP may contain extensions not listed in the profiles in this section only upon LM PMA approval.

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

All Issuer and Subject Names shall be Distinguished Names.

Issuer Unique Identifier and Subject Unique Identifier shall not be present.

For attribute values other than Domain Component (DC) and email address[6]: All CA Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as a printable string. All Certificate Holder DN portions to which name constraints apply shall be encoded as a printable string. Other portions of the Certificate Holder DN shall be encoded as a printable string if possible. If a portion cannot be encoded as a printable string, then and only then shall it be encoded using a different format, and that format shall be UTF8.

For DC and email address attribute values: All DC attribute values shall be encoded as an IA5 string.

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

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

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

Practice Note: If the Entity PKI leverages the CRL to provide revocation status for its delegated OCSP services, that CA should issue a full and complete CRL (i.e., a CRL without *issuingDistributionPoint* extension). This will ensure all revocation information is in one place and readily available to the OCSP Responder.

---

[6] Note that the LM PKI does not recommend using email address in a DN.

10.1 Cross-Certificate from LM Signing CA to Commercial Bridge Certification Authority (CBCA)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	Up to 3 years; expressed in UTCTime until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PKCS-10 request from the PCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
CRL Distribution Points[7]	c=no;
Certificate Policies	c=no; {1.3.6.1.4.1.103.100.1.1.3.4}, {1.3.6.1.4.1.103.100.1.1.3.3}, {1.3.6.1.4.1.103.100.1.1.3.6}, {1.3.6.1.4.1.103.100.1.1.3.7}
Policy Mapping	For SHA-2 cross-certs issued to the CertiPath SHA-2 Bridge CA: c=no; [{1.3.6.1.4.1.103.100.1.1.3.4} {1.3.6.1.4.1.24019.1.1.1.1}] [{1.3.6.1.4.1.103.100.1.1.3.3} {1.3.6.1.4.1.24019.1.1.1.2}] [{1.3.6.1.4.1.103.100.1.1.3.4} {1.3.6.1.4.1.24019.1.1.1.2}] [{1.3.6.1.4.1.103.100.1.1.3.6} {1.3.6.1.4.1.24019.1.1.1.24}] [{1.3.6.1.4.1.103.100.1.1.3.7} {1.3.6.1.4.1.24019.1.1.1.23}] [{1.3.6.1.4.1.103.100.1.1.3.7} {1.3.6.1.4.1.24019.1.1.1.24}] For SHA-2 cross-certs issued to the TSCP SHA-2 Bridge CA: c=no; [{1.3.6.1.4.1.103.100.1.1.3.4} {1.3.6.1.4.1.38099.1.1.1.1}] [{1.3.6.1.4.1.103.100.1.1.3.3} {1.3.6.1.4.1.38099.1.1.1.2}] [{1.3.6.1.4.1.103.100.1.1.3.4} {1.3.6.1.4.1.38099.1.1.1.2}] [{1.3.6.1.4.1.103.100.1.1.3.6} {1.3.6.1.4.1.38099.1.1.1.13}]
Basic Constraints	c=yes; CA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Directory Address="o=Lockheed Martin Corporation, c=US" Directory Address="DC=lmco, DC=com" RFC822 Name =lmco.com RFC822 Name=.lmco.com DNS Name=lmco.com DNS Name=lockheedmartin.com

Field	Value
Policy Constraints[8]	Optional. Either Absent or c=yes; requireExplicitPolicy, skipCerts = 0
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to LM Signing CA; id-ad-ocsp method entry contains HTTP URL for the LM Signing CA OCSP Responder
Certificate Template Name	c=no; CrossCA
Certificate Template Information	c=no; 'Template=LM Cross Certification Authority G2' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
Inhibit anyPolicy	c=no; skipCerts = 0

[7] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

[8] Inclusion of Policy Constraints in a cross certificate issued by the LM Signing CA to a CBCA is optional. If implemented, all certificates with a trust path that traverses the Commercial PKI Bridge must be valid for one or more mapped policies.

10.2 Lockheed Martin Off-line Root CA (also called Trust Anchor)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation, L=Denver, S=Colorado, C=US
Validity Period	Up to 20 years; expressed in UTCTime until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	CN= Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation, L=Denver, S=Colorado, C=US
Subject Public Key Information	Per Section 10.13
Extension	**Value**
Subject Key Identifier	c=no; Octet String
CA Version	c=no; V<CA certificate index>.<CRL and key index>
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonrepudiation (optional)
Basic Constraints	c=yes; cA=True; path length constraint absent

10.3 Intermediate or Signing CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation, L=Denver, S=Colorado, C=US
Validity Period	Expressed in UTCTime until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 Subject CA DN as specified in Section 7.1.4 of this CP i.e. CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Subject Public Key Information	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Root CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
CA Version	c=no; V<CA certificate index>.<CRL and key index>
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonrepudiation (optional)
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.3}, { 1.3.6.1.4.1.103.100.1.1.3.4}, { 1.3.6.1.4.1.103.100.1.1.3.5}, { 1.3.6.1.4.1.103.100.1.1.3.6}, { 1.3.6.1.4.1.103.100.1.1.3.7}
Certificate Template Name	c=no; SubCA
Basic Constraints [9]	c=yes; CA=True; path length constraint absent
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Root CA; id-ad-ocsp access method entry contains HTTP URL for the Root CA OCSP Responder (optional)
Subject Information Access	c=no; id-ad-caRepository (1.3.6.1.5.5.7.48.5) containing an HTTP URI pointing to a file that has an extension of .p7c. The file is a certs-only Cryptographic Message Syntax file (RFC 5751) that includes valid CA certificates issued by the subject CA. If the certificate asserts a path length constraint of zero in Basic Constraints, this extension may be omitted.
CRL Distribution Points[10]	c = no;

[9] In general, if a Signing CA is not used to cross-certify another entity's' CA, then the Basic Constraints path length constraint is set to zero

[10] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The

reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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 Certificate holder Certificates – Medium Level of Assurance

The following charts provide details for Certificate holder Certificates at the Medium Level of Assurance.

10.4.1 Certificate holder Identity Certificate – Medium Software

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; digitalSignature (required)
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.4}
Subject Alternative Name	c=no; UserPrincipalName (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance Software Identity - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[11]	c = no;
1.3.6.1.4.1.311.25.2	c = no; Octet String containing the AD-Object SID for the Subject

[11] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.4.2 Certificate holder Identity Certificate – Medium Hardware

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; digitalSignature (required)
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.3}
Subject Alternative Name	c=no; UserPrincipalName (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance HW Identity - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[12]	c = no;
1.3.6.1.4.1.311.25.2	c = no; Octet String containing the AD-Object SID for the Subject

[12] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.4.3 Certificate holder Signature Certificate – Medium Software

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.4}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance Software Digital Signature - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[13]	c = no;

[13] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and one, optionally, for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.4.4 Certificate holder Signature Certificate – Medium Hardware

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.3}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance HW Digital Signature - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[14]	c = no;

[14] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.4.5 Certificate holder Encryption Certificate – Medium Software

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.4}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance Software Encryption - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[15]	c = no;

[15] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.4.6 Certificate holder Encryption Certificate – Medium Hardware

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	No longer than 3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; per Section 10.12
Certificate Policies	c=no; { 1.3.6.1.4.1.103.100.1.1.3.3}
Subject Alternative Name	c=no; RFC822 email address (required); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
Certificate Template Information	c=no; 'Template=LM SHA2 Medium Assurance HW Encryption - US' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
CRL Distribution Points[16]	c = no;

[16] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.5 Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	Unique X.500 Signing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; expressed in UTCTime until 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	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=no; { 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; Applicable certificate policies
Subject Alternative Name	c=no; DN of the person controlling the code signing private key
CRL Distribution Points[17]	c = no;
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder

[17] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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).

10.6 Device or Server Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	Unique X.500 Signing CA DN as specified in Section 7.1.4 of this CP
Validity Period	3 years from date of issue; expressed in UTCTime until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP with O=Lockheed Martin Corporation, C=US prefix and with cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Key Usage	c=yes; RSA: keyEncipherment, digitalSignature ECC: digitalSignature (required)[18], keyAgreement (optional)
Extended key usage	c=no; per Section 10.12
Certificate Policies	c=no; Applicable certificate policies
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA; id-ad-ocsp access method entry contains HTTP URL for the Signing CA OCSP Responder
CRL Distribution Points[19]	c = no; always present
1.3.6.1.4.1.311.25.2	c = no; Octet String containing the AD-Object SID for the Subject

[18] TLS Servers and devices should use certificates for authentication and Ephemeral DH obviating the need for key agreement

[19] The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain up to three URIs, two for HTTP (i.e., of the form http://…) and, optionally, one for LDAP. The reasons and cRLIssuer fields shall not be populated. The CRL URI shall point to a full and complete CRL or a Distribution Point based partitioned CRL. In the case of 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 OCSP Responder Certificate

The following table contains the OCSP Responder certificate profile assuming that the OCSP Responder certificate is issued by the same CA using the same key as the Certificate holder Certificate. Alternative trust models such as OCSP Responder as trust anchor may be acceptable to the LM PMA.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	CN= Lockheed Martin Certification Authority 6 G3, OU=Certification Authorities, O=Lockheed Martin Corporation, C=US
Validity Period	120 days or less; expressed in UTCTime until 2049 and GeneralizedTime for dates thereafter
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN as specified in Section 7.1.4 of this CP with O=Lockheed Martin Corporation, C=US prefix
Subject Public Key Information	Per Section 10.13
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Signing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Signing CA)
Certificate Template Information	c=no; 'Template=LM CA4 OCSP Response Signing 2003 Manual' plus AD template object metadata (e.g object OID and Major/Minor version numbers)
Key Usage	c=yes; digitalSignature (required), nonrepudiation (optional)
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate Policies[20]	c=no; Applicable certificate policies
Subject Alternative Name	c=no; URI: HTTP URL for the OCSP Responder (preferred); and/or DNS: Fully qualified domain name of the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; optional; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Signing CA

10.8 PKCS 10 Request Format

The following table contains the format for PKCS 10 requests whose intended purpose is that of an Intermediate or Signing CA Certificate.

[20] This field shall contain all of the certificate policy OIDs for which the CA issues certificates.

Field	Value
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Per Section 10.13
Subject's Signature	Signed using the private key associated with above Subject Public Key
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC-822, and DNS name forms

10.9 CRL Format

10.9.1 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	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	Unique X.500 Signing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	Expressed in UTCTime until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	expressed in UTCTime until end of 2049 and GeneralizedTime for dates thereafter; (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
CRL Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CA Version	c=no; V<CA certificate index>.<CRL and key index>
CRL Number	c=no; monotonically increasing whole number (never repeated)
Next CRL Publish	c=no; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; (>= thisUpdate + CRL issuance frequency)
Freshest CRL	c=no; optional, distributionPoint field containing an HTTP URL pointing to the deltaCRL
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when revoked for key compromise or CA compromise

10.9.2 Distribution Point Based Partitioned CRL

The Entity PKI may make a distribution based partitioned CRL available to the relying parties in lieu of or in addition to the full and complete CRL. The distribution point based partition CRL shall adhere to the following profile. Note that the CRL may not be an indirect CRL, may not be partitioned based on reason codes, and may not assert a distribution point that is a nameRelativetoCRLIssuer.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; >= thisUpdate + CRL issuance frequency
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
CRL Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CA Version	c=no; V<CA certificate index>.<CRL and key index>
CRL Number	c=no; monotonically increasing whole number (never repeated)
Next CRL Publish	c=no; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; (>= thisUpdate + CRL issuance frequency)
Freshest CRL	c=no; optional, distributionPoint field containing an HTTP URL pointing to the deltaCRL
Issuing Distribution Point	c=yes; distribution point field must contain a full name (i.e., distribution point field may not contain nameRelativetoCRLIssuer; the following fields must all be absent: onlySomeReasons, indirectCRL, and onlyContainsAttributeCerts
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when revoked for key compromise or CA compromise

10.9.3 Delta CRL

The Entity PKI may make a delta-CRL available to the relying parties in addition to the full and complete CRL, so long as complete for scope CRLs are issued with sufficient frequency to meet the requirements specified in Section 4.9.7 of the Lockheed Martin Certificate Policy.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Issuer Distinguished Name	Unique X.500 Issuing CA DN as specified in Section 7.1.4 of this CP
thisUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter
nextUpdate	Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; >= thisUpdate + CRL issuance frequency
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter)
CRL Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CA Version	c=no; V<CA certificate index>.<CRL and key index>
CRL Number	c=no; monotonically increasing whole number (never repeated)
Next CRL Publish	c=no; Expressed in UTCTime for dates until end of 2049 and GeneralizedTime for dates thereafter; (>= thisUpdate + CRL issuance frequency)
Delta CRL Indicator	c=yes; monotonically increasing integer (never repeated)
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when revoked for key compromise or CA compromise

10.10 OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 6960 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	Must contain one and only one CertID
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.11 OCSP Response Format

See RFC 6960 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	Value
Response Status	As specified in RFC 6960
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	KeyHash as specified in RFC6960 (SHA-1 hash of the BIT STRING subjectPublicKey excluding the tag, length, and number of unused bits in the responder's certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[21], thisUpdate, nextUpdate[22],
Responder Signature	sha384 WithRSAEncryption {1 2 840 113549 1 1 12} sha512 WithRSAEncryption {1 2 840 113549 1 1 13}
Certificates	Applicable OCSP Responder certificate
Response Extension	**Value**
Nonce	(optional) c=no; Value in the nonce field of request (only included if present in the request)[23]
Response Entry Extension	**Value**
None	None

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

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

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

10.12 Extended Key Usage

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA[24]	None	None	All
Code Signing	id-kp-codesigning {1 3 6 1 5 5 7 3 3}	Life-time Signing {1.3.6.1.4.1.311.10.3.13}[25]	All Others
Domain Controller	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-pkinit-KPKdc {1 3 6 1 5 2 3 5}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}	None	All Others
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
Certificate Holder, Group, or Role, Identity Certificate	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}[26]	Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage and/or anyExtendedKeyUsage {2.5.29.37.0}
Certificate Holder, Group, or Role, Encryption Certificate[27]	id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	Any EKU that is not consistent with Key Usage and/or anyExtendedKeyUsage {2.5.29.37.0}

[24] CA certificate includes self-signed Root, cross certificates, subordinate CA certificates, and self-issued key rollover certificates.

[25] It is recommended that this EKU be included so that MSFT platforms will not verify signed code using an expired certificate.

[26] The last two only if the private key is in hardware.

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

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Certificate Holder, Group, or Role, Signature Certificate	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; MSFT Document Signing {1.3.6.1.4.1.311.10.3.12}	Adobe Certified Document Signing {1.2.840.113583.1.1.5}; Any EKU that is consistent with Key Usage	Any EKU that is not consistent with Key Usage and/or anyExtendedKeyUsage {2.5.29.37.0}
Time Stamp Authority	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	None	All Others
VPN Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others
VPN Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7417.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others
Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Web Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Workstation	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others

10.13 Subject Public Key Information Format

If the Subject Public Key is RSA, it shall be of the following format:

Algorithm OID: rsaEncryption {1 2 840 113549 1 1 1}
Parameters: NULL
Modulus m and public exponent e where,
m is 2048, 3072, or 4096 bits; and
$2^{16} < e < 2^{256}$

If the Subject Public Key is Elliptic Curve key, it shall be of the following format. This example assumes that P256 curve is used. See Section 7.1.3 for additional allowable curves.

Algorithm OID: ecPublicKey {1 2 840 10045 2 1},
Parameters: namedCurve P-256 {1 2 840 10045 3 1 7},
Subject Public Key: Uncompressed EC Point

10.14 Lockheed Martin Internal Certificate Templates

Lockheed Martin issues a number of certificate templates that are internal in nature and do not include any OIDs that are mapped to by any outside/external relying parties. These templates are not included in the CP text but the creation, configuration, and other details of each of these specific templates is detailed in the CertPS.

11 PKI REPOSITORY INTEROPERABILITY PROFILE

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

- Protocol
- Authentication
- Naming
- Object Class
- Attributes

Each of these items is described below.

11.1 Protocol

Lockheed Martin's PKI repository shall implement a system that provides HTTP protocol access to (CA) certificates and CRLs. Implementing the LDAPv3 protocol is optional.

11.2 Authentication

The PKI Repository shall permit "none" or "anonymous" authentication to read certificate and CRL information.

The PKI Repository shall permit "anonymous" authentication for browse and list operations, if those operations are supported.

For X.500 Directory Server System, a 'none' authentication shall be sufficient.

11.3 Naming

This CP has defined the naming convention.

When an LDAP repository is used:

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

11.4 Object Class

When an LDAP repository is used:

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

11.5 Attributes

When an LDAP repository is used:

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

12 BIBLIOGRAPHY

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

ANSI X9.62	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-03-11
ANSI X9.63 (R2017)	Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, 2001-11-20
CHARTER	CertiPath PMA Charter
FIPS 140	Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/PubsFIPS.html
FIPS 186	Digital Signature Standard, https://csrc.nist.gov/publications/fips
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors, https://csrc.nist.gov/publications/fips
RFC 2527	Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.
RFC 4210	Certificate Management Protocol, Adams Farrell et al, September 2005. http://www.ietf.org/rfc/rfc4210.txt.
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003. http://www.ietf.org/rfc/rfc3647.txt
LM PMA Charter	Lockheed Martin Public Key Infrastructure Policy Management Authority Charter For Operations
CertiPath CP	CertiPath Certificate Policy
RFC 4122	A Universally Unique Identifier (UUID) URN Namespace, Leach, Mealling, and Salz, July 2005 http://www.ietf.org/rfc/rfc4122.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper et. al., May 2008 http://www.ietf.org/rfc/rfc5280.txt
RFC 6712	Internet X.509 Public Key Infrastructure—HTTP Transfer for the Certificate Management Protocol (CMP) September 2012 https://www.ietf.org/rfc/rfc6712.txt

RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Santesson, Myers et. al., June 2013 http://www.ietf.org/rfc/rfc6960.txt
RFC 7292	PKCS #12: Personal Information Exchange Syntax v1.1 July 2014 https://www.ietf.org/rfc/rfc7292.txt
SP800-73	Interfaces for Personal Identity Verification, https://csrc.nist.gov/publications/sp800
SP800-76	Biometric Data Specification for Personal Identity Verification, https://csrc.nist.gov/publications/sp800
SP800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, https://csrc.nist.gov/publications/sp800

13 ACRONYMS & ABBREVIATIONS

AES	Advanced Encryption Standard
AGREEMENT	See 'MOA'
ANSI	American National Standards Institute
C	Country
CA	Certification Authority
CBCA	Commercial Bridge Certification Authority
CBP	Commercial Best Practices
CHUID	Cardholder Unique Identifier
CIMC	Certificate Issuing and Management Components
CISO	Corporate Information Security Office
CN	Common Name
CP	Certificate Policy
CertPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DDS	Data Decryption Server
DN	Distinguished Name
DNS	Domain Name Service
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End Entity
EKU	Extended Key Usage

GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISO	Information Security Operations
ITS	IT Solutions
KED	Key Escrow Database
KRA	Key Recovery Agent
KRO	Key Recovery Officer
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
KRS	Key Recovery System
LDAP	Lightweight Directory Access Protocol
LM PMA	Lockheed Martin Policy Management Authority
MOA	Memorandum of Agreement
MSA	Master Service Agreement (used when referencing the Certipath Agreement).
NIST	National Institute of Standards and Technology
O	Organization
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit

PCA	Principal Certification Authority
PI/PD	Personal Information/Personal Data
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCVP	Simple Certificate Validation Protocol
SHA-	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TSCP	Transglobal Secure Collaboration Program
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

14 GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
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 certificate holder is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
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.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
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.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its certificate holder, (3) contains the certificate holder's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.
Certificate Holder	A Certificate holder 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
Certification 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	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Certificate holder, (3) contains the Certificate holder's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to certificate holders.
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 (CertPS)	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 certificate holder's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority (CSA)	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
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.
Court of Competent Jurisdiction	Any court or forum that has the power and authority to properly exercise jurisdiction to interpret and/or enforce laws.
Credential	Evidence attesting to one's right to credit or authority; in this CP, it is any software- or hardware-based artifact and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
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. [FIPS1402]
Cryptoperiod	Time span during which each key setting remains in effect.
Customer	Any party that Lockheed Martin issues a certificate to and authorizes the use of that certificate in transactions
Data Decryption Server	An automated system that obtains subscriber private keys from the Key Escrow Database or other DDS in order to support decryption of data entering and leaving the Organization (e.g., encrypted email).
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 Certificate holders.
Enterprise CA	A CA operated by or on behalf of an organization for the primary purpose of issuing credentials to its own employees and other affiliated organizations.
Entity	An organization with operational control of a CA that will interoperate with a LM CA.
Entity CA	A CA that acts on behalf of an Entity and is under the operational control of an Entity.
Extended Key Usage	A certificate extension to further restrict the applications for which the public key in the certificate can be used.
Firewall	Gateway that limits access between networks in accordance with local security policy.
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. 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	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
Key Escrow Database	The function, system, or subsystem that maintains the key escrow repository and responds to key registration and key recovery requests from at least two Key Recovery Agents. It may also support subscriber automated self-recovery and automated recovery by a Data Decryption Server.
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.
Key Recovery	Production of a copy of an escrowed key and delivery of that key to an authorized requestor.
Key Recovery Agent	An individual authorized to interface with the key escrow database (in conjunction with one or more other Key Recovery Agents) to cause the key escrow database to carry out key recovery requests.
Key Recovery Officer	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of requestors.
Key Recovery Practice Statement	When utilized, a statement of the practices, procedures and mechanisms that a key recovery system employs in registering and recovering escrowed keys.
Key Recovery Requestor	An individual who is authorized to request recovery of a Subscriber's escrowed key. Subscribers may request recovery of their own keys.
Key Recovery Workstation	A dedicated workstation from which the Key Recovery Agent interfaces with the key escrow database.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Lockheed Martin Operational Authority (LM OA)	The LM Operational Authority is the organization selected by the LM PMA to be responsible for operating the LM offline rootCA and LM Signing CA.

Lockheed Martin Root Certification Authority (LMRCA)	The LM Root Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to issue certificates to Entity Principal Certification Authorities.
Lockheed Martin PMA	The Lockheed Martin PMA is a body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability.
Master Service Agreement	Agreement between LM and Certipath.
Memorandum of Agreement (MOA)	Agreement between the LM PMA and an Entity allowing interoperability between the Entity Principal CA and the LM 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.
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. 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.
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.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Repository	See Repository
PKI Sponsor	Fills the role of a Certificate holder for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Certificate holders as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the LM CA. An Entity may designate multiple Principal CA to interoperate with the LM CA.
Privacy	Restricting access to certificate holder 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).
Sunset Date	As used in this document, the expiration or termination date after which a specific provision is no longer permitted.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Supervised Remote Identity Proofing	A real-time identity proofing event where the RA/Trusted Agent is not in the same physical location as the applicant/Certificate Holder. The RA/Trusted Agent controls the device utilized by the applicant/Certificate Holder during the remote identity proofing

	process. The remote identity proofing process employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. Supervised Remote Identity Proofing must meet the criteria specified in Section 5.3.3 of NIST SP 800-63A, dated June 2017; and must have the capacity to capture an approved biometric when utilized for PIV-I credential issuance.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Certificate holder 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.

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.
Update (in reference to significant change)	Alterations to Licensed Software, including code and/or error corrections and minor code enhancements or modifications, that may be developed and generally released from time to time by the Software Vendor and made available to the customer (licensee). Software Updates do not include: (i) Software Upgrades of the Licensed Software that may be developed and generally released from time to time by the software vendor.
Upgrade (in reference to significant change)	Enhancements to the Licensed Software providing a new program feature or function that may be developed and generally released from time to time by the software vendor and made available to customer (licensee). Software Upgrades do not include: (i) Software Updates of the Licensed Software that may be developed and generally released from time to time by the software updates.
Wildcard Certificate	A single SSL/TLS certificate with a wildcard character (*) in the domain name field. This allows the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain.
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. [FIPS1402]